Dominion KX III

管理者ガイド
リリース 3.0.0

Copyright © 2014 Raritan, Inc.
DKX3A-v3.0.0-0B-J
2014 年 2 月
255-62-0002-00

本書には、著作権によって保護されている専有情報が含まれています。無断で転載することは禁じられており、本書のいかなる部分も、Raritan, Inc. より事前に書面による承諾を得ることなく複写、複製、他の言語へ翻訳することはできません。

© Copyright 2014 Raritan, Inc. 本書に記載されているサードパーティ製のすべてのソフトウェアおよびハードウェアは、それぞれの所有者の登録商標または商標であり、それぞれの所有者に帰属します。

FCC 情報

この装置は、FCC 規則のパート 15 に定められたクラス A デジタル装置に関する規制要件に基づき試験が実施され、その適合が認証されています。これらの規制要件は、商業環境において機器を使用する際、有害な干渉に対する妥当な保護を提供するために設けられています。この機器は、無線周波数エネルギーを生成かつ利用すると共に、放射することもあります。取扱説明書に従って設置および使用が行われない場合は、無線通信に有害な干渉を引き起こす恐れがあります。この機器を住宅地で利用すると有害な干渉を引き起こす場合もあります。

VCCI 情報 (日本)

この装置は，クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　VCCI－A

Raritan は、事故、災害、誤用、乱用、本製品の Raritan 製品以外への改良が起因する、または Raritan が適切にコントロールできないような状況下、もしくは通常の操作以外で発生した本製品への損傷に対して一切責任を負いません。

本製品に付属されている電源ケーブルは、本製品でのみ使用してください。

1F61
I.T.E.

ラック マウントの安全上のガイドライン

ラック マウントが必要なラリタン製品を使用する場合、以下のことに注意してください。

- 閉め切ったラック環境では、室温より高くなる場合があります。装置で指定された最高動作温度を超えないようにしてください。**仕様**を参照してください。
- ラック内に十分な空気の流れがあることを確認してください。
- 装置をラックにマウントする際は、機械的に安定して搭載されるように注意してマウントしてください。
- 回路に過大電流が流れないよう、装置を電源に接続する際は注意してください。
- 特に､電源タップ（直接接続を除く）など電力供給をはじめとするすべての装置を分岐回路に正しく接地してください。

目次

はじめに 1

概要...1
ヘルプでの最新情報...1
パッケージの内容...2
KX III の写真および機能...2
ハードウェア...2
ソフトウェア...3
Dominion KX3-832...4
Dominion KX3-864...6
モデルごとにサポートされているユーザ数とポート数...7
KX III リモート/ローカル コンソール インタフェース...7
KX III KVM Client アプリケーション...8
KX III オンライン ヘルプ...8

入門 9

KX III の設置および設定...9
ポップアップの許可...9
セキュリティ警告および検証メッセージ...9
Java 検証およびアクセス警告...9
その他のセキュリティ警告...10
証明書のインストール...10
例 1: ブラウザへの証明書のインポート...11
例 2: [信頼済みサイト] への KX III の追加と証明書のインポート...13
KX III へのログイン...14

KX III インタフェースおよびナビゲーション 16

概要...16
KX III リモート コンソール インタフェース...16
[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)...17
[Port Action] (ポート アクション) メニュー...20
左パネル...23
KX III コンソールでの案内...25

KX III ローカル コンソール インタフェース 26

KX III 管理者ヘルプ 27

概要 27
KX III の設置と設定 28
ラック マウント 28
デフォルトのログイン情報 29
手順 1: ネットワーク ファイアウォールの設定 30
手順 2: KVM ターゲット サーバの設定 30
手順 3: 装置の接続 34
手順 4: KX III の設定 37
手順 5: KX III リモート コンソールの起動 42
手順 6: キーボード言語の設定 (オプション) 44
手順 7: SSL 証明書の作成およびインストール 45
ラック PDU (電源タップ) のコンセントの制御 46
概要 46
コンセントの電源オン/オフの切り替えまたは電源再投入を行う 47
USB プロファイル 49
概要 49
CIM の互換性 49
使用できる USB プロファイル 50
KVM ポート用のプロファイルの選択 56
[User Management] (ユーザ管理) 57
ユーザ グループ 57
ユーザ 66
[Authentication Settings] (認証設定) 70
パスワードの変更 83
デバイス管理 84
ネットワーク設定 84
ポートの設定 89
[Device Services] (デバイス サービス) 134
[Power Supply Setup] (電源設定) 157
スクリプトの接続と切断 158
ポート グループ管理 164
デフォルトの GUI 言語設定の変更 168
セキュリティ上の問題 168
セキュリティの設定 168
IP アクセス制御を設定する 181
SSL 証明書 183
セキュリティ バナー 186
保守 188
[Audit Log] (監査ログ) 188
[Device Information] (デバイス情報) 190
バックアップと復元 192

[USB Profile Management] (USB プロファイルの管理) ... 195
CIM アップグレード ... 196
KX III ファームウェアのアップグレード ... 197
アップグレード履歴 ... 199
KX III の再起動 ... 199
CC-SG 管理の終了 ... 201
診断 ... 202
[Network Interface] (ネットワーク インタフェース) ページ ... 202
[Network Statistics] (ネットワーク統計) ページ ... 202
[ホストに ping する] ページ ... 205
[Trace Route to Host (ホストへのルートの追跡)] ページ ... 205
KX III 診断 ... 207
KX III ローカル コンソール ... 208
セキュリティと認証 ... 209
ローカル コンソールからの KX III ローカル ポートの設定 ... 209
コマンド ライン インタフェース (CLI) ... 214
概要 ... 214
CLI を使用しての KX III へのアクセス ... 215
KX III への SSH 接続 ... 215
ログイン ... 216
CLI の画面操作 ... 216
CLI を使用した初期設定 ... 218
CLI プロンプト ... 219
CLI コマンド ... 219
KX III コンソール サーバ設定用コマンドを使用する ... 220
ネットワークを設定する ... 221
デュアル ビデオ ポート グループ ... 223
デュアル ポート ビデオに関する推奨事項 ... 224
デュアル ビデオ ポート グループでサポートされているマウス モード ... 224
デュアル ビデオ サポートに必要な CIM ... 225
デュアル ポート ビデオ グループの使いやすさに関する注意事項 ... 226
権限およびデュアル ビデオ ポート グループ アクセス ... 227
デュアル ポート ビデオ グループ設定の例 ... 228
デュアル ビデオ ポート設定手順 ... 229
デュアル ビデオ ポート グループを使用する際の Raritan クライアントの画面操作 232
ダイレクト ポート アクセスおよびデュアル ポート ビデオ グループ ... 233
[Ports] (ポート) ページに表示されるデュアル ポート ビデオ グループ ... 233
LDAP スキーマを更新する ... 234
ユーザ グループ情報を返す ... 234
スキーマへの書き込み操作を許可するようにレジストリを設定する ... 235
新しい属性を作成する ... 235
属性をクラスに追加する ... 236
スキーマ キャッシュを更新する ... 238
ユーザ メンバの rciusergroup 属性を編集する ... 239

Virtual KVM Client (VKC) ヘルプ 242

概要....242
ターゲット サーバへの接続....243
接続プロパティの設定....244
接続プロパティへのアクセス....244
接続プロパティの概要....244
デフォルトの接続プロパティ設定 - 最適化による最高のパフォーマンスの実現....245
[Optimize for] (最適化): 選択....246
[Video Mode] (ビデオ モード)....246
[Noise Filter] (ノイズ フィルタ)....247
接続情報....248
接続情報のアクセスおよびコピー....249
USB プロファイル....249
キーボード....250
[Send Ctrl+Alt+Del] (Ctrl+Alt+Del の送信) マクロ....250
[Send LeftAlt+Tab] (Send LeftAlt+Tab の送信)....250
CIM キーボード/マウス オプションの設定....250
[Send Text to Target] (テキストをターゲットに送信)....251
キーボード マクロ....251
マクロの新規作成....251
マクロのインポート....253
マクロのエクスポート....254
ビデオのプロパティ....255
画面を更新する....255
[Auto-sense Video Settings] (ビデオ設定の自動検出)....256
色の調整....256
ビデオ設定の調整....256
ターゲット コマンドによるスクリーンショット (ターゲット スクリーンショット)....258
マウス オプション....259
デュアル マウス モード....260
シングル マウス モード....263
ツール オプション....263
[General Settings] (全般)....263
クライアント起動設定....266
VKC および AKC でのポート スキャンの設定....268
表示オプション....270
[View Toolbar] (ツール バーの表示)....270
[View Status Bar] (ステータス バーの表示)....270
[Scaling] (拡大、縮小)....270
[Full Screen Mode] (全画面モード)....271
仮想メディア....272
仮想メディアを使用するための条件....272
ローカル ドライブのマウント....273

仮想メディアによりサポートされているタスク 274
サポートされている仮想メディア タイプ 274
サポートされている仮想メディア オペレーティング システム 275
サポートされている仮想メディア ドライブ数 275
仮想メディアの接続および切断 276
Windows XP 環境での仮想メディア 278
Linux 環境での仮想メディア 279
Mac 環境での仮想メディア 279
仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ) 280
スマート カード 281
スマート カードの最小システム要件、CIM、およびサポートされているスマート カード リーダーとサポートされていないスマート カード リーダー 281
スマート カード リーダーへのアクセス時の認証 282
スマート カード使用時の PC 共有モードおよびプライバシー設定 282
スマート カード リーダーの検出 282
スマート カード リーダーのマウント 283
スマート カード リーダーの更新 283
スマート カードの取り外しおよび再挿入の通知の送信 284
スマート カード リーダーのアンマウント (取り外し) 284
デジタル音声 284
サポートされている音声デバイス形式 285
音声の再生とキャプチャに関する推奨事項と要件 285
音声レベル 285
PC 共有モードが有効になっている場合の音声接続に関する推奨事項 285
帯域幅要件 286
音声設定の保存 288
単一のリモート クライアントから複数のターゲットへの接続 288
デジタル音声デバイスの接続および切断 289
キャプチャ/再生バッファ サイズの調整 (音声設定) 292
バージョン情報 - Virtual KVM Client 292

Active KVM Client (AKC) ヘルプ 294

概要 294
ターゲット サーバへの接続 294
AKC でサポートされている Microsoft .Net Framework 295
AKC でサポートされているオペレーティング システム 295
AKC でサポートされているブラウザ 296
AKC を使用するため前提条件 296
Cookie を許可 296
"信頼済みサイト ゾーン" に KX III IP アドレスを追加 296
"保護モード" を無効化 296
AKC ダウンロード サーバ証明書の検証を有効にする 296

KX III ローカル コンソール - KX III エンド ユーザ ヘルプ 297

概要 ... 297
ターゲット サーバにアクセスする ... 297
ローカル コンソールの画面解像度 ... 298
ユーザが同時接続可能 ... 298
ホット キーと接続キー ... 299
KX III ローカル コンソール インタフェースへの切り替え - デフォルトのホット キー 299
接続キーの例 ... 299
Sun サーバへのアクセス時に使用できる特別なキー組み合わせ ... 301
ポートのスキャン - ローカル コンソール ... 302
ポートのスキャンのスライド ショー - ローカル コンソール ... 303
ポート スキャン中のターゲット ステータス インジケータ - ローカル コンソール .. 305
ローカル コンソール スキャンの設定 ... 305
ターゲットのスキャン - ローカル コンソール ... 306
ローカル コンソールのスマート カード アクセス ... 307
ローカル コンソールの USB プロファイル オプション ... 308
KX III ローカル コンソール ファクトリ リセット ... 309
デバイスのリセット ボタンによる KX III のリセット ... 310

KX III と Cat5 Reach DVI の接続 - 拡張ローカル ポート機能の提供 312

概要 ... 312
Cat5 Reach DVI の概要 ... 312
KX III と Cat5 Reach DVI の接続 ... 313

KX III から Paragon II へのアクセス 316

概要 ... 316
サポートされている Paragon II CIMS および設定 ... 317
KX III - KX III 構成の Paragon CIM に関するガイドライン ... 319
KX III - Paragon II 構成に関するガイドライン ... 320
Paragon II と KX III の間でサポートされている接続距離 ... 322
KX III への Paragon II の接続 ... 322

dcTrack での KX III の管理 324

概要 ... 324
キャビネット内の KX III 用スペースの検索 ... 325
dcTrack への KX III の追加 ... 326
手動による dcTrack への KX III の追加 ... 326
dcTrack への KX III のインポート ... 327
既存の KX III の複製 ... 328

KX III のデータ サーキットおよび電源サーキットの作成 328
KX III のアイテム追加要求の送信 329
KX III 作業工程の管理 329
キャビネット正面図およびフロア マップ図での KX III の可視化 329
KX III のライフサイクルの管理 331
KX III の移動 331
KX III の電源オン/オフ 331
KX III の有効化/有効化 331
KX III の使用停止と保管 331
KX III の使用停止とアーカイブ 331

仕様 332

ハードウェア 332
KX III の寸法および物理的仕様 332
KX III でサポートされているターゲット サーバ画面解像度 336
ターゲット サーバのサポートされている画面解像度、接続距離、およびリフレッシュ レート 337
KX III ローカル ポートのサポートされている DVI 解像度 338
サポートされているコンピュータ インタフェース モジュール (CIM) の仕様 338
サポートされているデジタル ビデオ CIM (Mac 用) 340
デジタル CIM タイミング モード 341
デジタル CIM の既定モードおよび標準モード 341
DVI 互換モード 342
サポートされているリモート接続 342
ネットワーク速度の設定 342
Dell 筐体を接続する場合のケーブル長と画面解像度 344
スマート カードの最小システム要件 344
サポートされているスマート カード リーダー 346
サポートされていないスマート カード リーダー 347
音声の再生とキャプチャに関する推奨事項と要件 348
サポートされている音声/仮想メディアおよびスマート カード接続の数 351
各言語に対して KX III でサポートされているキーボード 351
Mac Mini BIOS のキー入力コマンド 352
Windows キーボードによる Mac ターゲットへのアクセス 354
使用される TCP ポートおよび UDP ポート 354
ソフトウェア 355
サポートされているオペレーティング システムとブラウザ 355
Java および Microsoft .NET の要件 357
多言語対応キーボードの JRE の要件 357
監査ログおよび Syslog でキャプチャされるイベント 358

留意事項 359

概要......359
Java Runtime Environment (JRE) に関する留意事項......359
Java のキャッシュ機能の無効化および Java キャッシュのクリア......359
Java が Mac に正しくロードされていない場合......360
IPv6 のサポートに関する注意事項......361
オペレーティング システムの IPv6 のサポートに関する留意事項......361
AKC ダウンロード サーバ証明書検証の IPv6 サポートに関する留意事項......362
デュアル スタック ログインのパフォーマンスに関する問題......362
CIM に関する留意事項......362
Linux ターゲット サーバに対して Windows の 3 ボタン マウスを使用する場合......362
Windows 2000 での複合 USB デバイスの動作......363
仮想メディアに関する留意事項......364
Linux クライアントからドライブに接続できない場合......364
Mac クライアントからファイルの読み書きができない場合......364
Windows 環境での VKC および AKC を介した仮想メディア......365
ファイル追加後に仮想メディアが最新の情報に更新されない......366
仮想メディアの Linux ドライブが 2 回リストされる......366
Windows 2000 の仮想メディアへのアクセス......366
Mac および Linux の仮想メディア USB ドライブの切断......366
仮想メディア機能利用時におけるターゲット サーバの BIOS の起動時間......366
高速の仮想メディア接続を使用した場合の仮想メディアの接続エラー......367
USB ポートおよびプロファイルに関する留意事項......367
VM-CIM および DL360 の USB ポート......367
USB プロファイルの選択に関するヘルプ......367
スマート カード リーダー使用時の USB プロファイルの変更......369
ビデオ モードと解像度に関する留意事項......369
Mac でのビデオ画像の表示が暗い場合......369
ローカル ポートで黒色の縞が表示される場合......369
Sun Composite Sync ビデオ......369
SUSE と VESA のビデオ モード......370
キーボードに関する留意事項......370
フランス語キーボード......370
キーボード言語の設定 (Fedora クライアント)......372
Linux ターゲット サーバでマクロが保存されない場合......373
リモート アクセスに対応していない Mac キーボードのキー......374
マウスに関する留意事項......374
マウス ポインタの同期 (Fedora)......374
シングル マウス モード: CC-SG の管理下にあるターゲットに接続する場合......374
音声......375
音声の再生とキャプチャに関する問題......375
Linux 環境での音声......375
Windows 環境での音声......376

スマート カードに関する留意事項 376
Fedora サーバへの Virtual KVM Client (VKC) スマート カードの接続 376
CC-SG に関する留意事項 376
VKC のバージョンが CC-SG プロキシ モードで認識されない 376
デバイスのポート間の移動 376
ブラウザに関する留意事項 376
Fedora 使用時の Firefox のフリーズに関する問題の解決 376

FAQ 377

一般的な FAQ 377
リモート アクセス 380
ユニバーサル仮想メディア 384
帯域幅と KVM-over-IP のパフォーマンス 386
IPv6 ネットワーキング 390
サーバ 392
ブレード サーバ 393
インストール 395
ローカル ポート - KX III 397
拡張ローカル ポート 399
二重化電源 399
インテリジェント電源タップ (PDU) の管理 400
Ethernet と IP ネットワーキング 401
ローカル ポートの統合およびカスケード接続 403
コンピュータ インタフェース モジュール (CIM) 406
セキュリティ 407
スマート カード認証と CAC 認証 409
管理機能 410
ドキュメントおよびサポート 412
その他 413

索引 415

Ch 1 はじめに

この章の内容

概要..1
ヘルプでの最新情報...1
パッケージの内容...2
KX III の写真および機能..2
KX III リモート/ローカル コンソール インタフェース.........................7
KX III KVM Client アプリケーション 8
KX III オンライン ヘルプ 8

概要

Dominion KX III は､エンタープライズ クラスのセキュアな KVM-over-IP スイッチであり、1、2、4、または 8 ユーザが、8 ～ 64 台のサーバをリモート BIOS レベルで制御できます。

KX III は、DVI/HDMI/DisplayPort のデジタル/アナログ ビデオ、音声、仮想メディア、スマート カード/CAC、ブレード サーバ サポート、およびモバイル アクセスなどの標準機能を装備しています。

KX III を個々に、または Raritan の CommandCenter Secure Gateway (CC-SG) と共に導入します。

ヘルプでの最新情報

- KX III は DVI ビデオ モニタをサポート
- このリリースでは、以下の機能も追加:
  - Raritan の Cat5 Reach DVI への接続により KX III の接続距離を延長可能 - 「*KX III と Cat5 Reach DVI の接続 - 拡張ローカル ポート機能の提供* 『*312*p. 』」を参照
  - Virtual KVM Client (VKC) および Active KVM Client (AKC) の接続プロパティの変更 - 「*接続プロパティの設定* 『*244*p. 』」を参照
  - KX III リモート クライアントでのお気に入りの有効化/無効化 - 「お気に入りの管理」を参照
  - 外部のあらゆる仮想メディア ドライブ タイプをサポート

パッケージの内容

KX III は、標準 1U (kxx-864 の場合は 2U) 19 インチ ラックマウント シャーシに搭載される、完全に構成されたスタンドアロン製品として出荷されます。各 KX III は、以下の内容で出荷されます。

数量	品目
1	KX III
1	KX III クイック セットアップ ガイド
1	ラックマウント キット
2	AC 電源コード
1	ゴム足 1 組 (4 個、デスクトップ設置用)
1	アプリケーション ノート
1	保証書

KX III の写真および機能

ハードウェア

- KVM-over-IP リモート アクセスの統合
- 1U または 2U サイズ、ラックマウント対応、ブラケット付属
- フェイルオーバ対応の二重化電源 - 障害警告機能を備えた自動切換え電源
- 以下の CIM をサポート:
  - 仮想メディアおよびずれないマウスでは、次のいずれかの CIM を使用します。
    - D2CIM-VUSB
    - D2CIM-DVUSB
    - D2CIM-DVUSB-DVI
    - D2CIM-DVUSB-HDMI
    - D2CIM-DVUSB-DP
  - PS2 接続に必要:

  - DCIM-PS2
- DVI ローカル ポートから DVI モニタをサポート
  - DVI-VGA コンバータ経由の VGA サポート
  - 標準 DVI ケーブルによる DVI サポート
- 他の複数のカスケード接続デバイスへのアクセスに使用されるベース KX III デバイスでのカスケード接続のサポート
- マルチ ユーザ機能 (1/2/4/8 リモート ユーザ、1 ローカル ユーザ)
- UTP (Cat5/5e/6) ケーブルを使用したサーバへの配線
- フェイルオーバ対応の二重化 Ethernet ポート (10/100/1000 LAN)
- フィールド アップグレード可能
- ラック内アクセス用 USB ローカル ユーザ ポート
  - USB キーボード/マウス ポート
  - サポートされる USB デバイス用の USB ポート (前面に 1 ポート、背面に 3 ポート)
  - ローカル/リモート ユーザ アクセスと同時に操作可能
  - 管理用のローカル グラフィカル ユーザ インタフェース (GUI)
- 中央管理されるアクセス セキュリティ
- 電源管理の統合
- 二重化電源やネットワーク アクティビティ、リモート ユーザの状況を示す LED インジケータ
- ハードウェア リセット ボタン

注:リリース KX III 3.0.0 では、モデムがサポートされていませんが、今後のリリースでサポートされる予定です。

ソフトウェア

- Windows®、Mac®、および Linux® 環境での仮想メディア サポート*
- ずれないマウス*

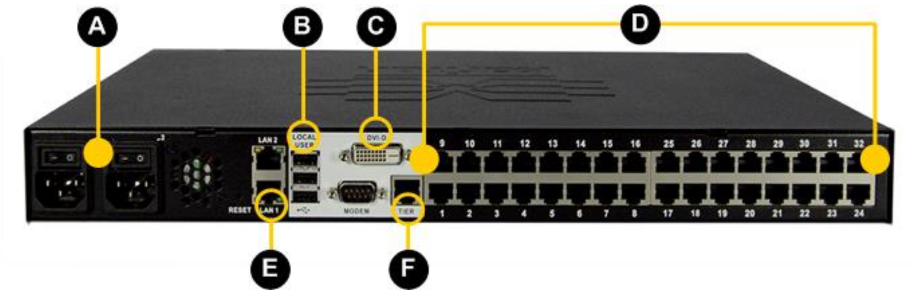
**注: 仮想メディアおよびずれないマウスには、D2CIM-VUSB、D2CIM-DVUSB、D2CIM-DVUSB DVI、D2CIM-DVUSB HDMI、または D2CIM-DVUSB-DP CIM を使用する必要があります。*

- USB を介したデジタル音声をサポート
- 設定可能なスキャン セット内で最大 32 台のターゲットをポートスキャンしサムネイル表示
- Web ベースのアクセスと管理
- わかりやすいグラフィカル ユーザ インタフェース (GUI)
- デュアル ポート ビデオ出力のサポート
- すべての KVM 信号を 256 ビット暗号化 (ビデオや仮想メディアを含む)
- LDAP、Active Directory®、RADIUS、または内部機能による認証および認可
- DHCP または静的な IP アドレスの指定
- スマート カード/CAC 認証
- SNMP、SNMP3、および Syslog 管理
- IPv4 および IPv6 のサポート
- 誤操作を防ぐためにサーバと直接関連付けられる電源管理
- Raritan の CommandCenter Secure Gateway (CC-SG) 管理ユニットとの統合
- CC-SG の制御からデバイスを解除するための CC Unmanage 機能
- Raritan PX1 および PX2 のアプライアンスのサポート

Dominion KX3-832

KX3-832 の写真

KX3-832 の特長



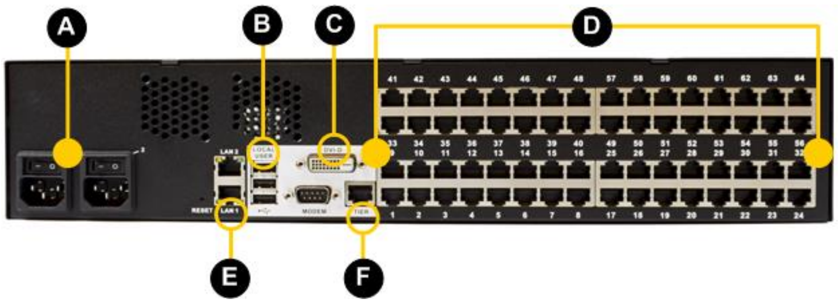
図の説明	
A	二重化電源 AC 100 V/240 V
B	ローカル USB ポート
C	DVI-D ポート
D	32 KVM ポート UTP ケーブル (Cat5/5e/6)
E	二重化 10/100/1000 Ethernet アクセス
F	カスケード接続ポート

注:リリース KX III 3.0.0 では、モデムがサポートされていませんが、今後のリリースでサポートされる予定です。

Dominion KX3-864

KX3-864 の写真

KX3-864 の特長



図の説明	
A	二重化電源 AC 100 V/240 V
B	ローカル USB ポート
C	DVI-D ポート
D	64 KVM ポート UTP ケーブル (Cat5/5e/6)
E	二重化 10/100/1000 Ethernet アクセス
F	カスケード接続ポート

図の説明
注:リリース KX III 3.0.0 では、モデムがサポートされていませんが、今後のリリースでサポートされる予定です。

モデルごとにサポートされているユーザ数とポート数

[Model] (モデル)	ポート	リモート ユーザ
KX3-864	64	8
KX3-832	32	8
KX3-808	8	8
KX3-464	64	4
KX3-432	32	4
KX3-416	16	4
KX3-232	32	2
KX3-216	16	2
KX3-132	32	1
KX3-116	16	1
KX3-108	8	1

KX III リモート/ローカル コンソール インタフェース

リモート コンソール インタフェースを使用して、ネットワーク接続経由で KX III の設定および管理を行います。

ローカル コンソール インタフェースでは、ローカルに KX III にアクセスできます。

それぞれ「*KX III リモート コンソール インタフェース* 『*16*p. 』」および「*KX III ローカル コンソール インタフェース* 『*26*p. 』」を参照してください。

KX III KVM Client アプリケーション

KX III は、Virtual KVM Client (VKC) および Active KVM Client (AKC) と連動します。

クライアントの使用法のヘルプについては、「*Virtual KVM Client (VKC) ヘルプ*『*242*p. 』」および「*Active KVM Client (AKC) ヘルプ*『*294*p. 』」を参照してください。

KX III オンライン ヘルプ

KX III オンライン ヘルプは、プライマリ ヘルプ ソースと見なされます。PDF バージョンのヘルプは、セカンダリ リソースです。

KX III を使用する前に、現在のリリースに関する重要な情報について、KX III リリース ノートを参照してください。

KVM Client ヘルプは、KX III オンライン ヘルプに含まれています。

オンライン ヘルプには、『KX III クイック セットアップ ガイド』が付属しています。これは、***Raritan の Web サイト***『***http://www.raritan.com/support/firmware-and-documentation*** 参照 』の「Raritan Firmware, Upgrades and Documentation」ページにあります。

「Raritan Firmware, Upgrades and Documentation」ページには、PDF バージョンのオンライン ヘルプのエンド ユーザ セクション (KVM Client ヘルプ、ローカル コンソール ヘルプ、リモート コンソール ヘルプ (該当する場合)、仕様など) も用意されています。も用意されています。

注:オンライン ヘルプを使用するには、ブラウザでアクティブ コンテンツを有効にする必要があります。

Ch 2　入門

この章の内容

KX III の設置および設定 9
ポップアップの許可 9
セキュリティ警告および検証メッセージ 9
証明書のインストール 10
KX III へのログイン 14

KX III の設置および設定

最初に使用する場合は、KX III を設置して設定します。

KX III に付属している、または *Raritan サポート Web サイト http://www.raritan.com/support* からダウンロードした『KX III クイック セットアップ ガイド』を参照するか、「*KX III の設置および設定* 『*28*p. の"*KX III の設置と設定*"参照 』」を参照してください。

ポップアップの許可

ブラウザの種類を問わず、KX III リモート コンソールを起動するためには、デバイスの IP アドレスからのポップアップを許可する必要があります。

セキュリティ警告および検証メッセージ

KX III にログインすると、セキュリティ警告およびアプリケーション検証メッセージが表示されることがあります。

この警告やメッセージには、以下のものがあります。

- Java™ セキュリティ警告および KX III の検証要求。「*Java 検証およびアクセス警告* 『*9*p. 』」および「*証明書のインストール* 『*10*p. 』」を参照してください。
- ブラウザおよびセキュリティの設定に基づくその他のセキュリティ警告。「*その他のセキュリティ警告* 『*10*p. 』」を参照してください。

Java 検証およびアクセス警告

KX III にログインすると、Java® 1.7 により、KX III を検証してアプリケーションへのアクセスを許可するよう求められます。

Java の警告を抑制し、セキュリティを強化するために、各 KX III に SSL 証明書をインストールすることをお勧めします。「*SSL 証明書* 『*183*p. 』」を参照してください。

その他のセキュリティ警告

KX III に SSL 証明書をインストールした後に、ブラウザおよびセキュリティの設定によっては、KX III にログインすると、さらにセキュリティ警告が表示される場合があります。

KX III リモート コンソールを起動するには、これらの警告を承諾する必要があります。

セキュリティと証明書に関する警告メッセージに対して以下のオプションをオンにすることにより、それ以降にログインしたときに表示される警告メッセージが抑制されます。

- [今後、この警告を表示しない]
- [この発行元からのコンテンツを常に信頼する]

証明書のインストール

ブラウザで、KX III の SSL 証明書を受け入れて検証するよう求められる場合があります。

ブラウザおよびセキュリティの設定によっては、KX III にログインすると、さらにセキュリティ警告が表示される場合があります。

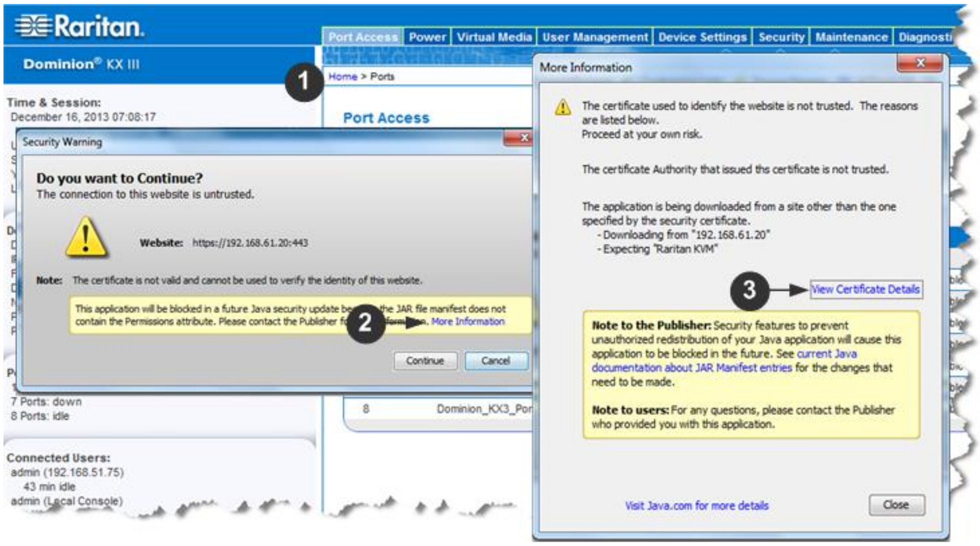
KX III リモート コンソールを起動するには、これらの警告を承諾する必要があります。詳細については、「***セキュリティ警告および検証メッセージ***『*9*p. 』」を参照してください。

ブラウザで SSL 証明書をインストールする方法について、例を 2 つ示します。どちらも Microsoft Internet Explorer 8® および Windows 7® を使用します。

具体的な方法および手順は、使用するブラウザおよびオペレーティング システムによって異なります。詳細については、使用するブラウザおよびオペレーティング システムのヘルプを参照してください。

例 1: ブラウザへの証明書のインポート

この例では、ブラウザに証明書をインポートします。

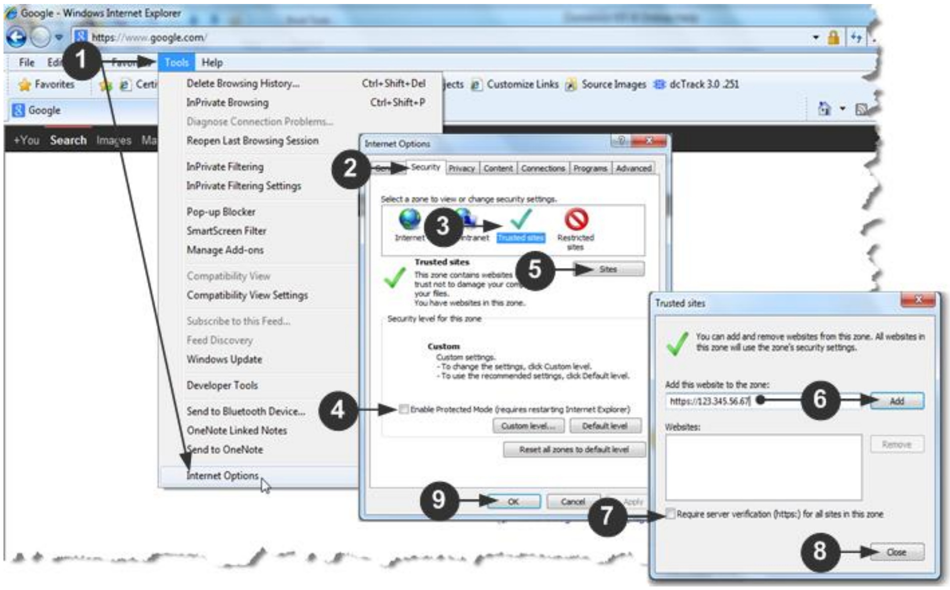


手順	
1	IE ブラウザを開き、KX III にログインします。
2	最初の Java™ セキュリティ警告で [More Information] (詳細情報) をクリックします。
3	[More Information] (詳細情報) ダイアログ ボックスで [View Certificate Details] (証明書の詳細の表示) をクリックします。証明書をインストールするかどうかを確認するダイアログ ボックスが開きます。ウィザードの手順に従います。 *注:ブラウザで確認が求められない場合は、手動で [ツール] の [インターネット オプション] を選択して、[インターネット オプション] ダイアログ ボックスを開きます。*

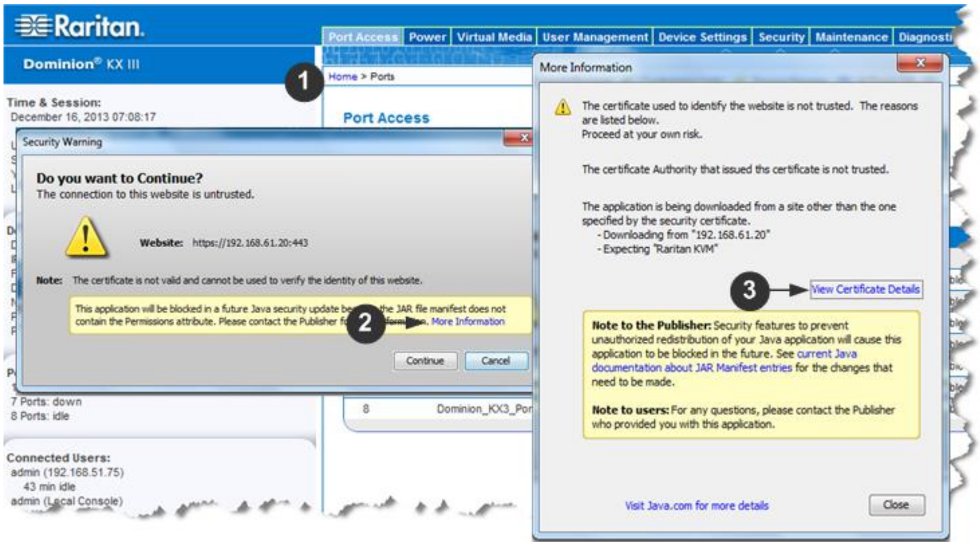
手順	
4	[コンテンツ] タブをクリックします。
5	[証明書] をクリックします。
6	証明書のインポート ウィザードが開くので、各手順を進めます。 ▪ [インポートする証明書ファイル] – 参照して証明書を探す ▪ [証明書ストア] – 場所を選択して証明書を保存する
7	ウィザードの最後の手順で [完了] をクリックします。
8	証明書がインポートされます。成功メッセージを閉じます。
9	[インターネット オプション] ダイアログ ボックスで [OK] をクリックして変更を適用し、ブラウザを閉じて再度開きます。

例 2: [信頼済みサイト] への KX III の追加と証明書のインポート

この例では、KX III の URL が信頼済みサイトとして追加され、一連の手続きの中で自己署名証明書が追加されます。



手順	
1	IE ブラウザを開き、[ツール] の [インターネット オプション] を選択して、[インターネット オプション] ダイアログ ボックスを開きます。
2	[セキュリティ] タブをクリックします。
3	[信頼済みサイト] をクリックします。
4	保護モードを無効にして、あらゆる警告を承諾します。
5	[サイト] をクリックして、[信頼済みサイト] ダイアログ ボックスを開きます。
6	KX III の URL を入力して、[追加] をクリックします。
7	このゾーンに対するサーバの確認を選択解除します (該当する場合)。
8	[Close] (閉じる) をクリックします。
9	[インターネット オプション] ダイアログ ボックスで [OK] をクリックして変更を適用し、ブラウザを閉じて再度開きます。 次に、証明書をインポートします。



手順	
1	IE ブラウザを開き、KX III にログインします。
2	最初の Java™ セキュリティ警告で [More Information] (詳細情報) をクリックします。
3	[More Information] (詳細情報) ダイアログ ボックスで [View Certificate Details] (証明書の詳細の表示) をクリックします。証明書をインストールするかどうかを確認するダイアログ ボックスが開きます。ウィザードの手順に従います。 詳細については、「*例 1: ブラウザへの証明書のインポート* 『*11*p. 』」を参照してください。

KX III へのログイン

Microsoft .NET® や Java Runtime Environment™ がインストールされており、ネットワーク接続機能を備えたワークステーションから KX III リモート コンソールにログインします。

KX III にログインして使用するには、ポップアップを許可する必要があります。

セキュリティ警告と検証メッセージ、およびそれらを抑制または除外する手順については、「*セキュリティ警告および検証メッセージ*『*9*p. 』」を参照してください。

▶ **KX III にログインするには、以下の手順に従います。**

1. サポートされている Web ブラウザを起動します。

2. 次のどちらかを入力します。
   - URL: *http://IP-ADDRESS*（Java ベースの Virtual KVM Client を使用する場合）

     または
   - *http://IP-ADDRESS/akc*（Microsoft .NET ベースの Active KVM Client の場合）

   IP-ADDRESS は、KX III に割り当てられた IP アドレスです。

   また、HTTPS を使用するか、管理者によって割り当てられた、KX III の DNS 名（適用可能な場合）を使用することもできます。

   常に、HTTP の IP アドレスから HTTPS の IP アドレスにリダイレクトされます。
3. ユーザ名とパスワードを入力して、[Login]（ログイン）をクリックします。
4. ユーザ同意書に承諾します（該当する場合)。
5. セキュリティ警告が表示される場合は、アクセスの承諾または許可、あるいはその両方を行います。

Ch 3　KX III インタフェースおよびナビゲーション

この章の内容

概要 16
KX III リモート コンソール インタフェース 16
KX III ローカル コンソール インタフェース 26

概要

KX III リモート コンソール インタフェースと KX III ローカル コンソール インタフェースは、デバイス設定および管理、ターゲット サーバのリストおよび選択用に、Web ベース インタフェースを備えています。

KX III リモート コンソール インタフェース

KX III リモート コンソールは、ブラウザ ベースのグラフィカル ユーザ インタフェースで、このコンソールを通じて、KX III に接続されている KVM ターゲット サーバおよびシリアル ターゲットにログインして、KX III をリモート管理できます。

KX III リモート コンソールは、接続されているターゲット サーバへのデジタル接続を提供します。KX III リモート コンソールを使用して KVM ターゲット サーバにログインすると、Virtual KVM Client のウィンドウが開きます。

KX III ローカル コンソールと KX III リモート コンソールのグラフィカル ユーザ インタフェースには多くの類似点があります。相違点については、ユーザ マニュアルに記載されています。以下のオプションは KX III リモート コンソールに用意されていますが、KX III ローカル コンソールには用意されていません。

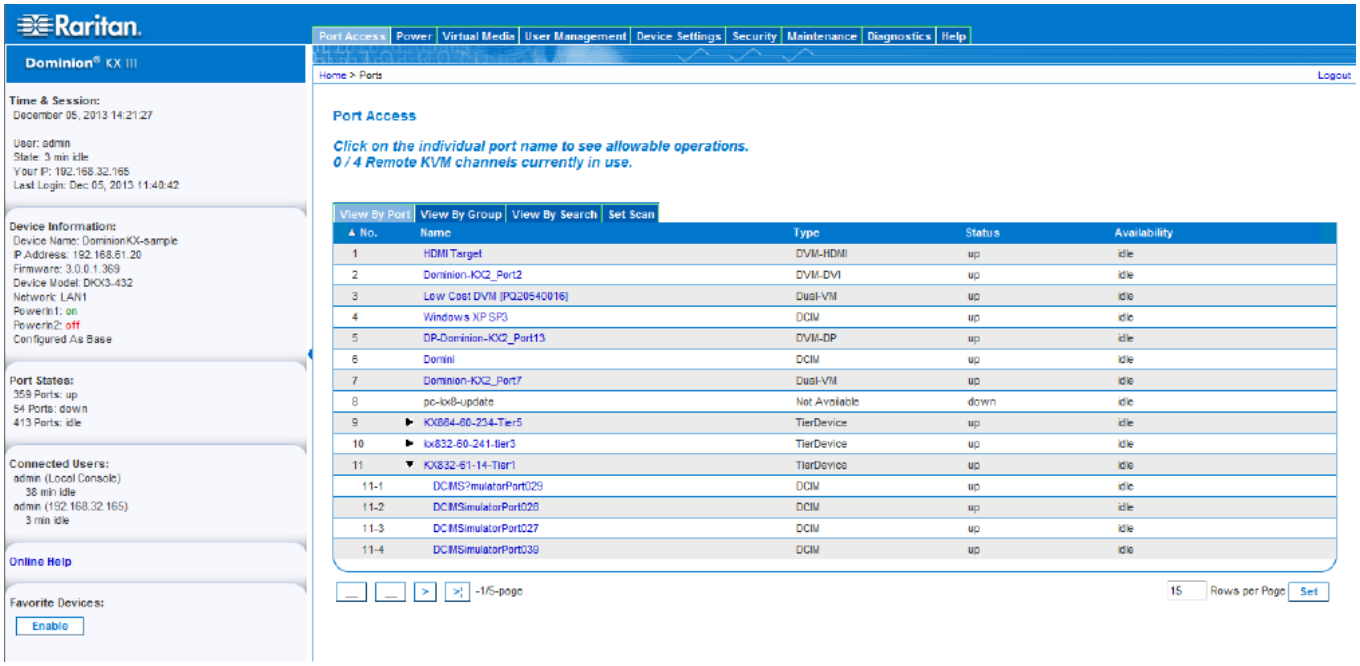
- 仮想メディア
- [Favorites] (お気に入り)
- [Backup/Restore] (バックアップ/リストア)
- [Firmware Upgrade] (ファームウェアのアップグレード)
- SSL 証明書
- 音声

[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)

正常にログインすると、[Port Access] (ポート アクセス) ページが表示され、すべてのポートについて、そのステータスと可用性が表示されます。

KVM ターゲット サーバ (ブレード サーバや標準サーバ) に接続されているポートは、青で表示されます。こうしたポートのいずれかを右クリックして、[Port Action] (ポート アクション) メニューを開きます。詳細については、「*[Port Action] (ポート アクション) メニュー*『*20*p. 』」を参照してください。

CIM が接続されていないか、CIM 名が空白になっているポートには、デフォルト ポート名「Dominion-KX3_Port#」が割り当てられます。「Port#」は KX III の物理ポートの番号を表します。



このページの 4 つのタブでは、ポート別の表示、グループ別の表示、検索による表示、およびポートのスキャンが可能です。

列の見出しをクリックすることで、ポート番号、ポート名、ステータス ([Up] (アップ) および [Down] (ダウン))、可用性 ([Idle] (アイドル)、[Connected] (接続済み)、[Busy] (ビジー)、[Unavailable] (使用不可能)、[Connecting] (接続中)) で並べ替えを行うことができます。

[Set Scan] (スキャン設定) タブを使用して、KX III に接続されているターゲットを 32 台までスキャンできます。「ポートのスキャン - リモート コンソール」を参照してください。

カスケード接続デバイス - [Port Access] (ポート アクセス) ページ

ティアー接続構成にしており、ベース KX III デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、 カスケード接続デバイスは、[ポート アクセス] ページでカスケード接続デバイス名の左にある展開矢印アイコン ► をクリックすると表示されます。カスケード接続の詳細については、「カスケード接続の設定および有効化」を参照してください。

ブレード シャーシ - [Port Access] (ポート アクセス) ページ

ブレード サーバは、[Port Access] (ポート アクセス) ページ上の展開可能な階層リストに表示されます。階層のルートはブレード シャーシで、個別のブレードはルートの下にラベルが付けられて表示されます。個別のブレードを表示するには、ルート シャーシの横の展開矢印アイコン ► を使用します。

注: ブレード シャーシを階層順に表示するには、ブレード サーバ シャーシにブレード シャーシのサブタイプを設定する必要があります。

デュアル ビデオ ポート グループ - [Port Access] (ポート アクセス) ページ

デュアル ビデオ ポート グループは、[Port Access (ポート アクセス)] ページにデュアル ポート タイプとして表示されます。ポート グループに属しているプライマリ ポートおよびセカンダリ ポートは、[Port Access (ポート アクセス)] ページに、それぞれ [Dual Port(P) (デュアル ポート (P))] および [Dual Port(S) (デュアル ポート (S))] として表示されます。たとえば、CIM タイプが DCIM の場合は、[DCIM Dual Port (P) (DCIM デュアル ポート (P))] が表示されます。

リモート クライアントからデュアル ポート ビデオ グループにアクセスする場合は、プライマリ ポートに接続すると、デュアル ポート グループのプライマリ ポートとセカンダリ ポートの両方に対する KVM 接続ウィンドウが開きます。

注: デュアル ビデオ プライマリ ポートは、ポート グループの作成時に定義されます。

注: プライマリ ポートのクリックによってデュアル ビデオ ポート グループにリモート接続するには、2 つの KVM チャネルが必要です。2 つのチャネルを利用できない場合、接続リンクは表示されません。

注: デュアル ビデオ ポート グループのセカンダリ ポートをクリックしても、[Action] (アクション) メニューは表示されません。

注: ローカル ポートからプライマリ ポートおよびセカンダリ ポートに同時に接続することはできません。

[View by Group] (グループ別表示) タブ

[View by Group] (グループ別表示) タブには、ブレード シャーシ、「標準の」ポート グループ、およびデュアル ビデオ ポート グループが表示されます。グループの横の展開矢印アイコン ▶ クリックすると、ポート グループに割り当てられたポートが表示されます。

こうしたタイプの各ポート グループの作成方法については、「デバイス管理」を参照してください。

[View by Search] (検索して表示) タブ

[View by Search] (検索して表示) タブでは、ポート名で検索できます。検索時にアスタリスク (*) をワイルドカードとして使用できます。また、名前全体で検索することも名前の一部だけで検索することもできます。

[Set Scan] (スキャン設定) タブ

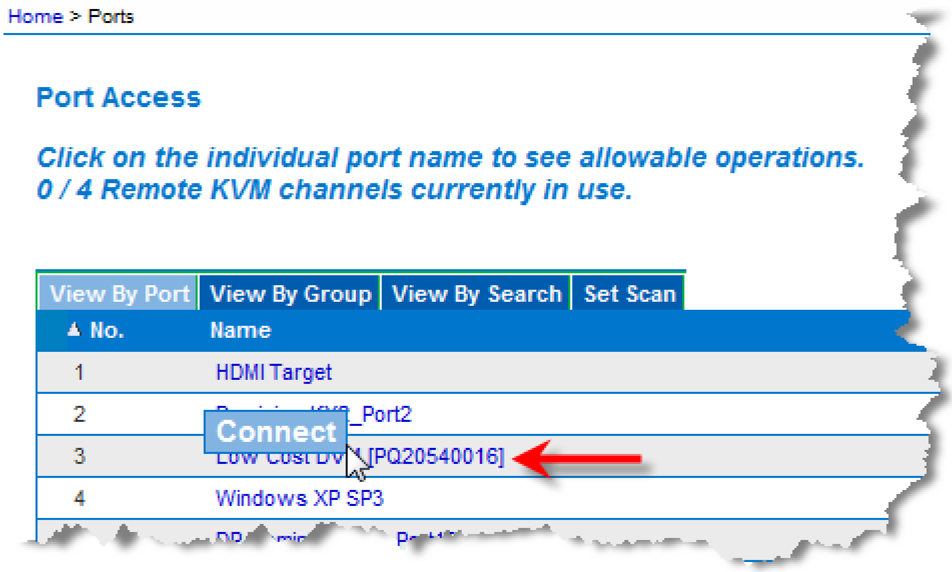
ポート スキャン機能には、[Port Access] (ポート アクセス) ページの [Set Scan] (スキャン設定) タブからアクセスします。この機能によって、スキャンするターゲットのセットを定義できます。スキャンしたターゲットのサムネイル表示も使用できます。サムネイルを選択すると、そのターゲットが Virtual KVM Client ウィンドウに表示されます。

「ポートのスキャン - リモート コンソール」を参照してください。

[Port Action] (ポート アクション) メニュー

[Port Access] (ポート アクセス) リストで [Port Name] (ポート名) をクリックすると、[Port Action] (ポート アクション) メニューが表示されます。

対象のポートに対して適切なメニュー オプションを選択して実行します。[Port Action] (ポート アクション) メニューには、ポートのステータスと可用性に応じて、その時点で利用可能なオプションだけが表示されます。



[Connect] (接続)

- [Connect] (接続) – ターゲット サーバへの新しい接続を作成します。

  KX III リモート コンソールの場合は、新しい Virtual KVM Client ページが表示されます。

  KX III ローカル コンソールの場合は、ローカル ユーザ インタフェースからターゲット サーバに表示が切り替わります。

  ローカル ポートで切り替えを行うためには、KX III ローカル コンソール インタフェースが表示されている必要があります。

  ローカル ポートからのホット キー切り替えも利用できるようになりました。

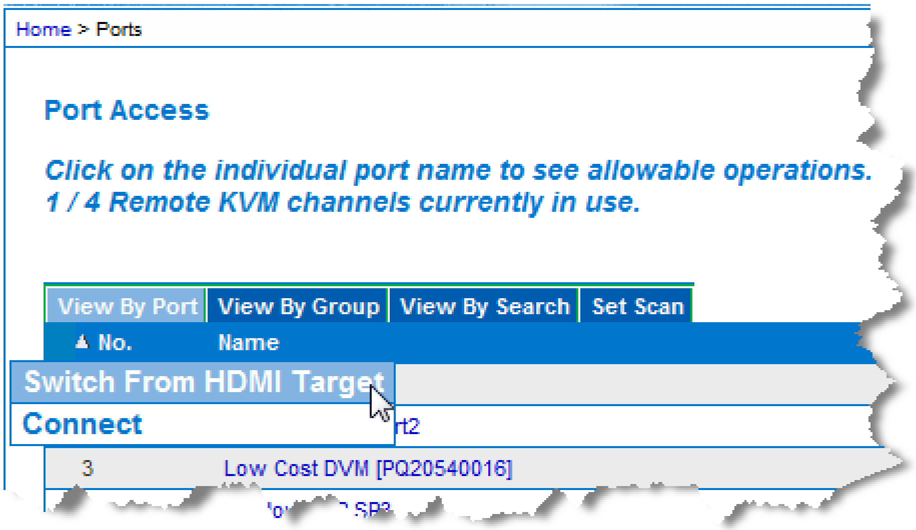
  注:すべての接続がビジー状態の場合、KX III リモート コンソールで使用可能なポートに対してこのオプションは使用できません。

[Switch From] (切り替え)

- [Switch From] (切り替え元) – 既存の接続から選択したポート (KVM ターゲット サーバ) に切り替えます。

  このメニュー項目は、KVM ターゲットに対してのみ、また Virtual KVM Client が開いている場合にのみ使用できます。

  注: KX III ローカル コンソールでは、このメニュー項目は使用できません。

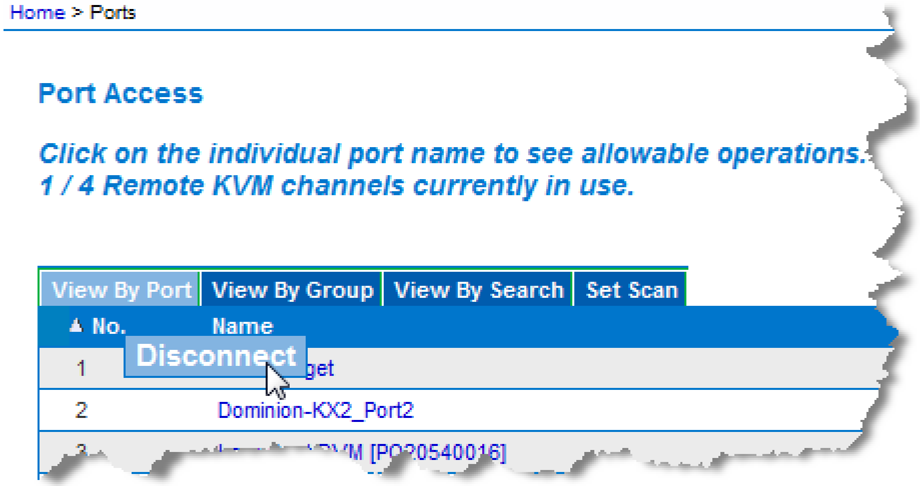


[Disconnect] (切断)

- [Disconnect] (切断) – このポートを切断し、このターゲット サーバの Virtual KVM Client ページを閉じます。

  このメニュー項目は、ポート ステータスが [up] (アップ) および [connected] (接続済み) であるか、または [up] (アップ) および [busy] (ビジー) であるときにのみ使用できます。

注: KX III ローカル コンソールでは、このメニュー項目は使用できません。ローカル コンソールで切り替えたターゲットを切断する唯一の方法は、ホットキーを使用することです。



[Power On] (電源オン)

- [Power On] (電源オン) – 関連付けられているコンセントを介してターゲット サーバの電源をオンにします。

  このオプションは、1 つ以上の電源がターゲットに関連付けられているとき、およびこのサービスを操作する許可がユーザに与えられているときにのみ表示されます。

[Power Off] (電源オフ)

- [Power Off] (電源オフ) – 関連付けられているコンセントを介してターゲット サーバの電源をオフにします。

  このオプションは、1 つ以上の電源がターゲットに関連付けられているとき、ターゲットがオン (ポート ステータスが [up] (アップ)) のとき、およびこのサービスを操作する許可がユーザに与えられているときにのみ表示されます。

[Power Cycle] (電源の再投入)

- [Power Cycle] (電源の再投入) – 関連付けられているコンセントを介してターゲット サーバの電源をいったんオフにしてから再びオンにします。

  このオプションは、1 つ以上の電源がターゲットに関連付けられているとき、およびこのサービスを操作する許可がユーザに与えられているときにのみ表示されます。

左パネル

KX III インタフェースの左パネルにある情報は次のとおりです。

一部の情報は、特定の条件に従って、つまり役割や利用する機能などに基づいて表示されます。各情報が表示される条件もこの表に示します。

情報	説明	表示される条件
[Time & Session] (日時およびセッション)	現在のセッションを開始した日時	常時
ユーザ	ユーザ名。	常時
[State] (状態)	アプリケーションの現在の状態 (アイドルまたはアクティブ)。アイドル状態の場合、セッションがアイドル状態になっている時間が追跡および表示されます。	常時
[Your IP] (あなたの IP アドレス)	KX III にアクセスする際に使用された IP アドレス	常時
[Last Login] (最終ログイン日時)	最後にログインした日時	常時
[Under CC-SG Management] (CC-SG の管理下)	KX III を管理している CC-SG デバイスの IP アドレス	KX III が CC-SG の管理下にある場合
[Device Information] (デバイス情報)	使用している KX III に特有の情報	常時
[Device Name] (デバイス名)	デバイスに割り当てられている名前	常時
IP アドレス	KX III の IP アドレス	常時
[Firmware] (ファームウェア)	ファームウェアの現在のバージョン	常時
[Device Model] (デバイス モデル)	KX III のモデル。	常時
[Serial number] (シリアル番号)	KX III のシリアル番号。	常時

情報	説明	表示される条件
ネットワーク	現在のネットワークに割り当てられている名前	常時
[PowerIn1] (電源入力 1)	電源コンセント 1 の接続状態 オンまたはオフ、あるいは自動検出オフ	常時
[PowerIn2] (電源入力 2)	電源コンセント 2 の接続状態 オンまたはオフ、あるいは自動検出オフ	常時
[Configured As Base] (ベース デバイスとして設定) または [Configured As Tiered] (カスケード接続デバイスとして設定)	カスケード接続を使用している場合、現在アクセスしている KX III がベース デバイスとカスケード接続デバイスのどちらであるかが表示されます。	KX III がカスケード接続構成の一要素になっている場合
ポートの状態	KX III によって現在使用されているポートのステータス	常時
[Connect Users] (接続しているユーザ)	現在 KX III に接続している、ユーザ名と IP アドレスによって識別されるユーザ	常時
オンライン ヘルプ	オンライン ヘルプへのリンク	常時
お気に入りデバイス	「お気に入りの管理」を参照	有効になっている場合
[FIPS Mode] (FIPS モード)	FIPS モード: 有効、SSL 証明書: FIPS モード準拠。	FIPS が有効になっている場合

左パネルの折りたたみ

左パネルを折りたたんで、ページの表示領域を拡大することができます。

▶ 左パネルを折りたたむには、以下の手順に従います。

- パネルの左側のほぼ中ほどにある青色の左向き矢印をクリックします。パネルが折りたたまれたら、青色の矢印をもう一度クリックすると展開されます。

KX III コンソールでの案内

KX III コンソール インタフェースでは、いくつかの方法でナビゲーションや選択を行うことができます。

▶ オプションを選択するには、以下のいずれかの手順に従います。

- タブをクリックします。利用可能なオプションのページが表示されます。
- タブ上にカーソルを移動し、メニューから適切なオプションを選択します。
- 表示されるメニュー階層（階層リンク）からオプションを直接クリックします。

▶ 画面に収まらないページをスクロールするには、以下のいずれかの手順に従います。

- キーボードの Page Up キーと Page Down キーを使用します。
- 右側にあるスクロール バーを使用します。

KX III ローカル コンソール インタフェース

KX III ローカル コンソールと KX III リモート コンソールのグラフィカル ユーザ インタフェースには、多くの類似点があります。相違点については、ヘルプに記載されています。

ローカル コンソールの使用法の詳細については、「*KX III ローカル コンソール－KX III エンド ユーザ ヘルプ*『*297*p.』」を参照してください。

Ch 4 KX III 管理者ヘルプ

この章の内容

概要 27
KX III の設置と設定 28
ラック PDU (電源タップ) のコンセントの制御 46
USB プロファイル 49
[User Management] (ユーザ管理) 57
デバイス管理 84
セキュリティ上の問題 168
保守 188
診断 202
KX III ローカル コンソール 208
コマンド ライン インタフェース (CLI) 214
デュアル ビデオ ポート グループ 223
LDAP スキーマを更新する 234

概要

管理者ヘルプでは、一般に KX III アプリケーション管理者によって実行される KX III 機能に特有の情報 (KX III の設置および設定、ユーザ グループおよびユーザの管理、セキュリティの管理など) を取り上げています。

通常、管理者機能は、KX III リモート コンソールやローカル コンソールから実行されます。

一般に Virtual KVM Client または Active KVM Client を使用してエンドユーザによって実行される機能、およびリモート コンソールまたはローカル コンソールから実行される一部の機能については、ヘルプの固有のセクションでそれぞれ説明されています。

こうした機能には、仮想メディアの使用、マウスの設定、スキャン ポート機能の使用、ビデオ オプションの設定などがあります。

KX III の設置と設定

基本的な最低限のセットアップ手順のクイック リファレンスについては、デバイスに付属する『KX III クイック セットアップ ガイド』を参照するか、Raritan のサポート Web サイトからガイドをダウンロードしてください。

QSG に記載されておらず、ここで取り上げられている追加情報やオプションの手順は、以下のとおりです。

- *サポートされているマウスの追加設定* 『*31*p. 』
- *KX III 起動中の LED ステータス* 『*34*p. 』
- *VGA モニタへの接続（オプション）*『*36*p. 』
- *手順 6: キーボード言語の設定（オプション）*『*44*p. 』

ラック マウント

KX III は、標準の 19 インチ機器用ラックの 1U（4.4 cm、1.75 インチ）のスペースに取り付けることができます。

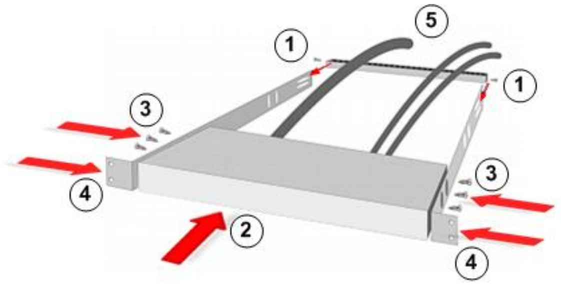
注:ラック マウントの図に描かれている Raritan デバイスは、例として挙げているにすぎず、お使いのデバイスと異なる場合があります。マウント手順は、お使いのデバイスによって特定されます。

前向きの取り付け

各手順は、前面ラック マウント図に示されている番号に対応しています。

1. 付属の 2 本のネジを使用して側面ブラケットの後端にケーブル支持バーを固定します。
2. KX III を、背面パネルがケーブル支持バーに面した状態で側面ブラケットの間にはめ込み、その前面パネルを側面ブラケットの「耳」に揃えます。
3. 残りのネジ（各側面に 3 本）を使用して、KX III を側面ブラケットに固定します。
4. アセンブリ全体をラックに取り付け、専用のネジ、ボルト、ケージ ナットなどで側面ブラケットの耳をラックの前面レールに固定します。

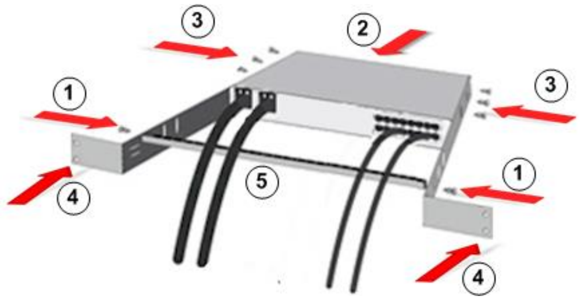
5. KX III の背面のパネルにケーブルを接続する場合は、ケーブルをケーブル支持バーに掛けます。



後向きの取り付け

各手順は、背面ラック マウント図に示されている番号に対応しています。

1. 付属の 2 本のネジを使用して側面ブラケットの前端に（側面ブラケットの「耳」の近くに）ケーブル支持バーを固定します。
2. KX III を、背面パネルがケーブル支持バーに面した状態で側面ブラケットの間にはめ込み、その前面パネルを側面ブラケットの後端に揃えます。
3. 残りのネジ（各側面に 3 本）を使用して、KX III を側面ブラケットに固定します。
4. アセンブリ全体をラックに取り付け、専用のネジ、ボルト、ケージ ナットなどで側面ブラケットの耳をラックの前面レールに固定します。
5. ユーザ ステーションまたはスイッチの背面のパネルにケーブルを接続する場合は、ケーブルをケーブル支持バーに掛けます。



デフォルトのログイン情報

デフォルト設定	値
ユーザ名	*admin* このユーザは、管理者特権を有します。
パスワード	*(「raritan」) を入力します。*

デフォルト設定	値
	KX III を初めて起動したときは、デフォルトのパスワードを変更する必要があります。
IP アドレス	192.168.0.192.

重要: バックアップと事業の継続性のためには、バックアップ管理者用のユーザ名およびパスワードを作成し、その情報を安全な場所に保管しておくことを強くお勧めします。

手順 1: ネットワーク ファイアウォールの設定

TCP ポート 5000

TCP ポート 5000 でのネットワークとファイアウォールの通信を許可すると、KX III へのリモート アクセスが有効になります。

あるいは、別の TCP ポートを使用するよう KX III を設定すると、そのポートで通信できるようになります。

TCP ポート 443

TCP ポート 443 (標準 HTTPS) へのアクセスを許可すると、Web ブラウザ経由で KX III にアクセスできるようになります。

TCP ポート 80

TCP ポート 80 (標準 HTTP) へのアクセスを許可すると、HTTP 要求が自動的に HTTPS にリダイレクトされます。

手順 2: KVM ターゲット サーバの設定

ターゲット サーバ画面解像度

サポートされているターゲット サーバ画面解像度については、「*KX III でサポートされているターゲット サーバ画面解像度* 『*336*p. 』」KX III オンライン ヘルプの を参照してください。

マウスの設定

ずれないマウス モードを利用して、ターゲット サーバでのマウス設定を最小限に抑えることをお勧めします。その他のマウス モードについては、 「*サポートされているマウスの追加設定* 『*31*p. 』」を参照してください。

このモードでは、ターゲット マウスの加速または速度が異なる値に設定されている場合でも、クライアントとターゲットのカーソルを同期するために絶対座標が使用されます。

このモードは USB ポートを備えたサーバでサポートされ、仮想メディア CIM のデフォルトのモードです。

ずれないマウス モード では、仮想メディア CIM を使用する必要があります。

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

サポートされているマウスの追加設定

これらの設定は、特に明記していない限り、ターゲット オペレーティング システムで設定されます。

マウスの設定

各種オペレーティング システムのマウス設定を以下に示します。

これらの設定は、特に明記していない限り、ターゲット オペレーティング システムで設定されます。

こうしたマウスの設定の詳細については、KX III のオンライン ヘルプまたはユーザ ガイドを参照してください。

Windows 7 および Windows Vista のマウス設定

▶ Windows 7® および Windows Vista® でのマウスの設定:

速度の設定を行います。

- ポインタの速度設定をちょうど中間の速度に設定する
- [ポインタの精度を高める] チェックボックスをオフにする

アニメーション効果とフェード効果を無効にします。

- [Windows 内のアニメーション コントロールと要素]
- [ウィンドウを最大化や最小化するときにアニメーションで表示する]
- [メニューをフェードまたはスライドして表示する]
- [ヒントをフェードまたはスライドで表示する]
- [メニュー項目をクリック後にフェード アウトする]

Windows XP、Windows 2003、Windows 2008 のマウス設定

▶ Windows XP®、Windows 2003®、および Windows 2008® でのマウスの設定:

速度の設定を行います。

- ポインタの速度設定をちょうど中間の速度に設定する
- [ポインタの精度を高める] チェックボックスをオフにする
- [動作] のオプションを無効にする

アニメーション効果を無効にします。

- [次のアニメーション効果をメニューとヒントに使用する] オプションをオフにする

Windows 2000 のマウス設定

▶ Windows 2000® でのマウスの設定:

速度の設定を行います。

- アクセラレーションを [なし] に設定する
- ポインタの速度設定をちょうど中間の速度に設定する

アニメーション効果を無効にします。

- [次のアニメーション効果をメニューとヒントに使用する] オプションをオフにする

Apple Mac のマウス設定

▶ Apple Mac® でのマウスの設定:

Mac® オペレーティング システムが稼動している KVM ターゲット サーバでマウスを正しく同期させるには、ずれないマウス機能が必要です。

ずれないマウス機能を正常に動作させるには、仮想メディア CIM が必要です。サポートされている CIM については、「***サポートされているコンピュータ インタフェース モジュール (CIM) の仕様*** 『*338*p. 』」を参照してください。

KX III の設置が完了したら、Mac USB プロファイルを設定します。このプロファイルを設定しない場合、OS X でマウスの同期が行われます。

次のいずれかの手順を実行します。

1. Raritan KVM Client から Mac ターゲットに接続します。
2. [USB Profile] (USB プロファイル)、[Other Profiles] (他のプロファイル)、[Mac OS-X (10.4.9 and later)] (Mac OS-X (10.4.9 以降)) の順に選択します。

   または

3. KX III で、[Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択し、ターゲット名をクリックして [Port] (ポート) ページを開きます。
4. [Select USB Profiles for Port] (ポートの USB プロファイルの選択) セクションを展開します。
5. [Available] (利用可能)ボックスから [Mac OS-X (10.4.9 and later)] (Mac OS-X (10.4.9 以降)) を選択し、[Add] (追加) をクリックして [Selected] (選択) ボックスに追加します。
6. [Selected] (選択) ボックスの [Mac OS-X (10.4.9 and later)] (Mac OS-X (10.4.9 以降)) をクリックします。これにより、選択したプロファイルが [Preferred Profile] (優先プロファイル) ドロップダウンに自動的に追加されます。
7. [Preferred Profile] (優先プロファイル) ドロップダウンから [Mac OS-X (10.4.9 and later)] (Mac OS-X (10.4.9 以降)) を選択し、[Set Active Profile As Preferred Profile] (アクティブ プロファイルを優先プロファイルとして設定) のチェックボックスをオンにします。

- [OK] をクリックして適用します。

Linux のマウス設定

▶ Linux® でのマウスの設定:

- (標準マウス モードのみ) マウスの加速値を正確に 1 に設定し、しきい値も正確に 1 に設定します。コマンド「`xset mouse 1 1`」を入力します。このコマンドは、ログイン時の実行用に設定する必要があります。

Sun Solaris のマウス設定

▶ **Sun® Solaris™ でのマウスの設定:**

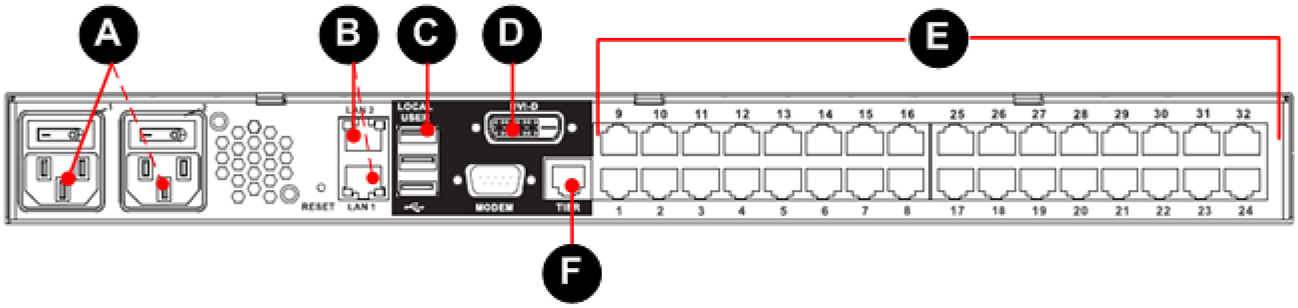
- マウスの加速値を正確に 1 に設定し、しきい値も正確に 1 に設定する
- ビデオ カードの解像度が、サポートされている値に設定されており、出力が VGA (Composite Sync 以外) であることを確認する

IBM AIX のマウス設定

▶ **IBM AIX® でのマウスの設定:**

- [Style Manager] を開き、[マウスの設定] をクリックして、[マウスの加速] を 1.0 に設定し、[しきい値] を 3.0 に設定する

手順 3: 装置の接続



A. AC 電源:

▶ **電源の接続:**

1. 付属の AC 電源コードを KX III と AC 電源コンセントに接続します。
2. 二重化電源フェイルオーバ保護を実装するには、付属の 2 つ目の AC 電源コードを KX III と、1 つ目の電源コードとは別の電源コンセントに接続します。

KX III 起動中の LED ステータス

KX III を起動すると、LED ライトは、次のようになります。

- 最初の電源投入時:
  - すべてのチャネル LED が点灯
  - 電源 LED が消灯
- 起動段階:
  - すべてのチャネル LED が消灯
  - 両方の電源がオンの場合、電源 LED は青色
  - 片方の電源がオンの場合、電源 LED は赤色

B. ネットワーク ポート

KX III には、負荷分散用ではなく、フェイルオーバ用の 2 つの Ethernet ポートが用意されています。

デフォルトでは LAN1 のみがアクティブで、自動フェイルオーバは無効になっています。

接続先の KX III の内蔵ネットワーク インタフェースまたはネットワーク スイッチが利用できなくなった場合に、LAN2 で同じ IP アドレスが使用されるようにするには、ネットワーク フェイルオーバを有効にします。

▶ **ネットワークに接続するには、以下の手順に従います。**

1. 標準 Ethernet ケーブルを、「LAN1」のラベルの付いたネットワーク ポートから、Ethernet スイッチ、ハブ、またはルータに接続します。
2. オプションの KX III Ethernet フェイルオーバ機能を使用するには、以下の手順に従います。
   a. 標準 Ethernet ケーブルを、「LAN2」のラベルの付いたネットワーク ポートから、Ethernet スイッチ、ハブ、またはルータに接続します。
   b. KX III の [Network Configuration] (ネットワーク設定) ページで [Enable Automatic Failover] (自動フェイルオーバを有効にする) をオンにします。

C. ローカル ユーザ ポート (ローカル コンソール)

▶ **キーボードおよびマウスを接続するには、以下の手順に従います。**

- USB キーボードおよびマウスを KX III の背面のそれぞれのローカル ユーザ ポートに接続します。

ラックに配置されている管理用およびターゲット サーバ アクセス用の KX III ローカル ユーザ ポートをグラフィカル ユーザ インタフェースを介して使用します。

ローカル ユーザ ポートは、設置およびセットアップの際に必要ですが、それ以降の使用を省略できます。

D. ローカル DVI-D ポート

標準 DVI ケーブルは、ローカル DVI モニタまたはキーボード トレイ (KX III には非付属) への接続に使用されます。

Raritan の T1700-LED キーボード トレイの DVI ポートに接続します。

必須の DVI-D-VGA コンバータを使用して VGA モニタに接続します。

DVI モニタへの接続

ローカル モニタは、1024 x 768 以上の解像度をサポートする必要があります。

▶ **DVI モニタに接続するには、以下の手順に従います。**

1. USB キーボードおよびマウスを KX III の背面のそれぞれのローカル ユーザ ポートに接続します。
2. DVI ケーブルの片側を KX III の背面の DVI-D ポートに接続します。
3. DVI ケーブルの反対側を DVI モニタの DVI ポートに接続します。

VGA モニタへの接続 (オプション)

▶ **VGA モニタに接続するには、以下の手順に従います。**

1. USB キーボードおよびマウスを KX III の背面のそれぞれのローカル ユーザ ポートに接続します。
2. DVI-D-VGA コンバータを KX III の背面の DVI-D ポートに接続し、両側のねじを時計回りに回してコンバータを固定します。
3. VGA ケーブルの片側を DVI-D-VGA コンバータに接続して、反対側を VGA モニタに接続し、ねじを締めてケーブルを固定します。

注:DVI-D-VGA コンバータは、KX III には付属していません。詳細については、Raritan の営業担当にお問い合わせください。

E. KX III へのターゲット サーバの接続

▶ **ターゲット サーバを KX III に接続するには、以下の手順に従います。**

1. CIM のキーボード、マウス、ビデオの各プラグをターゲット サーバの対応するポートに接続します。
2. CIM を KX III の背面の使用可能なターゲット サーバ ポートに Cat5/5e/6 ケーブルで接続します。

F. カスケード接続 (オプション)

「*カスケード接続を設定および有効化する* 『*135*p. , *http://www.raritan.com/help/kx-iii/v3.0.0/en/index.htm#33184*』」を参照してください。

手順 4: KX III の設定

以下の手順では、デフォルトのパスワードを変更し、ローカル コンソールで KX III にその IP アドレスを割り当てる必要があります。

他の手順はすべて、ローカル コンソールから実行するか、サポートされている Web ブラウザ経由で KX III のデフォルト IP アドレスを使用して KX III リモート コンソールから実行できます。

Java® 1.7 (以降) または Microsoft .NET® 3.5 (以降) では、KX III を使用する必要があります。.

デフォルト パスワードを変更する

KX III を初めて起動したときは、デフォルトのパスワードを変更する必要があります。

▶ **デフォルトのパスワードを変更するには、以下の手順に従います。**

1. ユニットが起動したら、デフォルトのユーザ名 *admin* およびパスワード *raritan* を入力します。[Login] (ログイン) をクリックします。
2. 古いパスワード *raritan* を入力して、新しいパスワードを入力し、もう一度入力します。

   パスワードには、最大 64 文字の英数字と特殊文字を使用できます。
3. [Apply] (適用) をクリックします。確認ページで [OK] をクリックします。

KX III への IP アドレスの割り当て

▶ **KX III に IP アドレスを割り当てるには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. KX III デバイスにわかりやすいデバイス名を指定します。

   最大 32 文字の英数字と有効な特殊文字を組み合わせて使用できます。スペースは使用できません。
3. 次に、IPv4、IPv6、および DNS を設定します。

IPv4 の設定

1. [IPv4] セクションで、適切な IPv4 固有のネットワーク設定を入力するか選択します。
   a. 必要な場合は、[IP Address] (IP アドレス) を入力します。デフォルトの IP アドレスは「192.168.0.192」です。
   b. [Subnet Mask] (サブネット マスク) を入力します。デフォルトのサブネット マスクは「255.255.255.0」です。

c. [IP Auto Configuration] (IP 自動設定) ドロップダウン リストで [None] (設定しない) を選択する場合は、[Default Gateway] (デフォルト ゲートウェイ) を入力します。

d. [IP Auto Configuration] (IP 自動設定) ドロップダウン リストで [DHCP] を選択する場合は、[Preferred DHCP Host Name] (優先 DHCP ホスト名) を入力します。

e. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。

- [None] (設定しない) (静的 IP) - このオプションを選択した場合は、ネットワークの IP アドレスを手動で指定する必要があります。

  KX III はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、このオプションを推奨します。

  プライマリ Ethernet ポート (またはそのポートに接続されているスイッチ/ルータ) に障害が発生したときに冗長フェイルオーバ機能を確実に作動させたい場合は、このオプションを選択します。プライマリ Ethernet ポートに障害が発生した場合、KX III は、同じ IP アドレスでセカンダリ ネットワーク ポートにフェイルオーバされるため、中断が生じることはありません。

- [DHCP] - DHCP サーバから一意の IP アドレスとその他のパラメータを取得するために、ネットワークに接続しているコンピュータ (クライアント) によって Dynamic Host Configuration Protocol が使用されます。

  このオプションを選択した場合、ネットワーク パラメータは DHCP サーバによって割り当てられます。

  DHCP を使用する場合は、[Preferred host name] (優先ホスト名) を入力します (DHCP のみ)。最大 63 文字まで使用できます。

2. 次に、IPv6 や DNS を設定します。

IPv6 の設定

1. IPv6 を使用する場合は、[IPv6] セクションで、適切な IPv6 固有のネットワーク設定を入力するか、選択します。

   a. [IPv6] チェックボックスをオンにしてセクション内のフィールドを有効にし、デバイスの IPv6 を有効にします。

   b. [Global/Unique IP Address] (グローバル/一意の IP アドレス) を入力します。これは、KX III に割り当てられる IP アドレスです。

   c. [Prefix Length] (固定長) を入力します。これは、IPv6 アドレスで使用されるビット数です。

   d. [Gateway IP Address] (ゲートウェイ IP アドレス) を入力します。

e. [Link-Local IP Address] (リンク - ローカル IP アドレス)。このアドレスは、デバイスに自動的に割り当てられ、近隣ノードを検出する場合や、ルータが存在しない場合に使用されます。**[Read-Only] (読み取り専用)**

f. [Zone ID] (ゾーン ID)。アドレスが関連付けられているデバイスを識別します。**[Read-Only] (読み取り専用)**

g. [IP Auto Configuration] (IP 自動設定) オプションを選択します。

- [None] (設定しない) (静的 IP) - このオプションを選択した場合は、ネットワークの IP アドレスを手動で指定する必要があります。

  KX III はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、このオプションを推奨します。

  プライマリ Ethernet ポート (またはそのポートに接続されているスイッチ/ルータ) に障害が発生したときに冗長フェイルオーバ機能を確実に作動させたい場合は、このオプションを選択します。プライマリ Ethernet ポートに障害が発生した場合、KX III は、同じ IP アドレスでセカンダリ ネットワーク ポートに切り替わるため、中断が生じることはありません。

  [None] (設定しない) が選択されている場合は、[Network Basic Settings] (ネットワーク基本設定) の次のフィールドが有効になります。([Global/Unique IP Address] (グローバル/一意の IP アドレス)、[Prefix Length] (固定長)、[Gateway IP Address] (ゲートウェイ IP アドレス)) が有効になり、IP アドレスを手動で設定できるようになります。

- [Router Discovery] (ルータ検出) - このオプションを使用して、直接接続されるサブネットにのみ適用される [Link Local] (リンク ローカル) を超える [Global] (グローバル) または [Unique Local] (一意ローカル) を意味する IPv6 アドレスを自動的に割り当てます。

2. 次に、DNS を設定します。

DNS の設定

1. [DHCP] が選択され、[Obtain DNS Server Address] (DNS サーバ アドレスを取得) が有効になっている場合は、[Obtain DNS Server Address Automatically] (DNS サーバ アドレスを自動的に取得) を選択します。DNS サーバ アドレスが自動的に取得されると、DHCP サーバが提供する DNS 情報が使用されます。
2. [Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用) を選択する場合は、[DHCP] が選択されているかどうかにかかわらず、このセクションに入力されたアドレスが、DNS サーバへの接続に使用されます。

[Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用) を選択する場合は、次の情報を入力します。これらのアドレスは、停電によりプライマリ DNS サーバ接続が切断された場合に使用されるプライマリおよびセカンダリ DNS アドレスです。

a. [Primary DNS Server IP Address] (プライマリ DNS サーバ IP アドレス)

b. [Secondary DNS Server IP Address] (セカンダリ DNS サーバ IP アドレス)

3. 完了したら [OK] をクリックします。

これで、KX III デバイスはネットワークにアクセスできます。

ターゲット サーバの命名

▶ ターゲット サーバに名前を付けるには、以下の手順に従います。

1. まだすべてのターゲット サーバを接続していない場合は、接続します。
2. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択し、名前を付けるターゲット サーバの [Port Name] (ポート名) をクリックします。
3. サーバの名前を入力します。

   最大 32 文字の英数字と特殊文字で指定します。
4. [OK] をクリックします。

電源の自動検出の指定

KX III には二重化電源が搭載されています。

両方の電源が使用されている場合は、どちらも KX III で自動的に検出され、それぞれのステータスが通知されます。

さらに、[Power Supply Setup] (電源設定) ページの [Powerln1 Auto Detect] (Powerln1 自動検出) と [Powerln2 Auto Detect] (Powerln2 自動検出) のチェックボックスがどちらも自動的にオンになります。

1 つの電源しか使用していない場合は、使用されている電源のみの自動検出を有効にすることができます。

▶ 使用中の電源の自動検出を有効にするには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Power Supply Setup] (電源設定) を選択します。[Power Supply Setup] (電源設定) ページが開きます。
2. 電源入力を 1 番目の電源 (デバイス背面の左端の電源) に接続している場合は、[Powerln1 Auto Detect] (Powerln1 自動検出) チェック ボックスをオンにします。

3. 電源入力を 2 番目の電源（デバイス背面の右端の電源）に接続している場合は、[Powerln2 Auto Detect]（Powerln2 自動検出）チェック ボックスをオンにします。
4. [OK] をクリックします。

どちらかのチェックボックスがオンで、電源入力のみが接続されている場合は、デバイス前面の電源 LED が赤色で点灯します。

日付/時刻の設定 (オプション)

必要に応じて、日付と時刻を設定します。

日付と時刻の設定は、LDAPS が有効になっている場合に SSL 証明書の検証に影響します。

▶ 日付と時刻を設定するには、以下の手順に従います。

1. [Device Settings]（デバイス設定）の [Date/Time]（日付/時刻）を選択します。[Date/Time Settings]（日付/時刻の設定）ページが開きます。
2. [Time Zone]（タイム ゾーン）ドロップダウン リストから適切なタイム ゾーンを選択します。
3. 夏時間用の調整を行うには、[Adjust for daylight savings time]（夏時間用の調整）チェックボックスをオンにします。
4. 日付と時刻の設定に用いる方法を選択します。
   - [User Specified Time]（ユーザによる時刻定義）- 日付と時刻を手動で入力する場合に、このオプションを使用します。[User Specified Time]（ユーザによる時刻定義）オプションを選択した場合は、日付と時刻を入力します。時刻は、hh:mm の形式を使用します（24 時間制で入力します）。
   - [Synchronize with NTP Server]（NTP サーバと同期）- 日付と時刻をネットワーク タイム プロトコル（NTP）サーバと同期するには、このオプションを選択します。
5. [Synchronize with NTP Server]（NTP サーバと同期）オプションを選択した場合は、以下の手順に従います。
   a. [Primary Time server]（プライマリ タイム サーバ）の IP アドレスを入力します。
   b. [Secondary Time server]（セカンダリ タイム サーバ）の IP アドレスを入力します。<オプション>

注:[Network]（ネットワーク)ページの [Network Settings]（ネットワーク設定）で [DHCP] が選択されている場合、NTP サーバ IP アドレスは、デフォルトでは DHCP サーバから自動的に取得されます。

NTP サーバ IP アドレスを手動で入力するには、[Override DHCP]（DHCP を無効にする）チェックボックスをオンにします。

---

6. [OK] をクリックします。

ユーザ グループとユーザの作成

CC-SG ユーザへの注意事項

CommandCenter Secure Gateway を使用して KX III を制御している場合、ローカル ポート アクセスを必要とするローカル ユーザを除き、ユーザおよびグループは CC-SG によって認証されます。

CC-SG で KX III を制御している場合、ローカル ポート ユーザは、KX III 上で設定されているローカル ユーザ データベースまたはリモート認証サーバ (LDAP/LDAPS または RADIUS) に対して認証され、CC-SG ユーザ データベースに対して認証されません。

CC-SG 認証の詳細については、『**CommandCenter Secure Gateway ユーザ ガイド**』、『**CommandCenter Secure Gateway 管理者ガイド**』、または『**CommandCenter Secure Gateway デプロイメント ガイド**』を参照してください。これらは、***Raritan の Web サイト http://www.raritan.com*** の「Support」セクションからダウンロードできます。

サポートされているプロトコル

ユーザ名とパスワードの管理を容易にするため、KX III には認証要求を外部認証サーバへ転送する機能があります。LDAP/LDAPS と RADIUS の 2 つの外部認証プロトコルがサポートされています。

Microsoft Active Directory についての注意事項

Microsoft® Active Directory® は、LDAP/LDAPS プロトコルをネイティブに使用し、LDAP/LDAPS サーバおよび KX III の認証元として機能することが可能です。IAS (インタフェース認可サーバ) のコンポーネントを装備している場合、Microsoft Active Directory サーバは、RADIUS 認証元としても機能します。

手順 5: KX III リモート コンソールの起動

Microsoft .NET® や Java Runtime Environment® がインストールされており、ネットワーク接続機能を備えたワークステーションから KX III リモート コンソールにログインします。

▶ **KX III リモート コンソールを起動するには、以下の手順に従います。**

1. サポートされている Web ブラウザを起動します。
2. 次のどちらかを入力します。
   - URL: *http://IP-ADDRESS* (Java ベースの Virtual KVM Client を使用する場合)

     または
   - *http://IP-ADDRESS/akc* (Microsoft .NET ベースの Active KVM Client の場合)

IP-ADDRESS は、KX III に割り当てられた IP アドレスです。

また、HTTPS を使用するか、管理者によって割り当てられた、KX III の DNS 名（適用可能な場合）を使用することもできます。

3. 常に、HTTP の IP アドレスから HTTPS の IP アドレスにリダイレクトされます。
4. ユーザ名とパスワードを入力します。[Login]（ログイン）をクリックします。

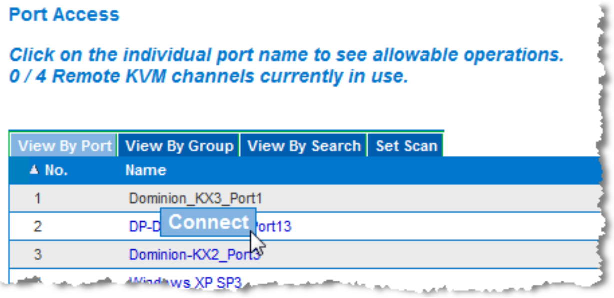
リモートからのターゲット サーバのアクセスと制御

KX III の [Port Access]（ポート アクセス）ページには、すべての KX III ポートの他に、接続中のターゲット サーバ、およびその状態と可用性が表示されます。

KX III からターゲット サーバへのアクセス

► **ターゲット サーバにアクセスするには、以下の手順に従います。**

1. KX III の [Port Access]（ポート アクセス）ページで、アクセスするターゲット サーバのポート名をクリックします。[Port Action]（ポート アクション）メニューが開きます。



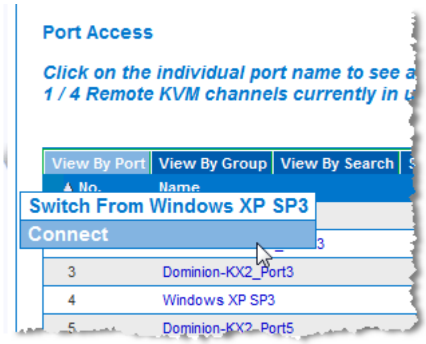
2. [Port Action]（ポート アクション）メニューの [Connect]（接続）をクリックします。[KVM] ウィンドウが開き、ターゲットへの接続が示されます。

ターゲット サーバを切り替える

► **KVM ターゲット サーバを切り替えるには、以下の手順に従います。**

1. ターゲット サーバを使用しているときに、KX III の [ポート アクセス] ページを開きます。
2. アクセスするターゲットの [ポート名] をクリックします。[ポート アクション] メニューが表示されます。

3. ［ポート アクション］メニューの［切り替え元］を選択します。選択した新しいターゲット サーバが表示されます。



ターゲット サーバの切断

▶ ターゲット サーバを切断するには、以下の手順に従います。

- [Port Access]（ポート アクセス）ページで、切断するターゲットのポート名をクリックし、表示される［Port Action］（ポート アクション）メニューの［Disconnect］（切断)をクリックします。

  または

- KVM Client ウィンドウを閉じます。

手順 6: キーボード言語の設定 (オプション)

注:英語（アメリカ)/インターナショナル キーボードを使用している場合は、この手順を実行する必要はありません。

英語（アメリカ）以外の言語を使用する場合は、該当する言語のキーボードを設定する必要があります。

また、クライアント マシンおよび KVM ターゲット サーバのキーボード言語を同じにする必要があります。

キーボード レイアウトを変更する方法の詳細については、お使いのオペレーティング システムのマニュアルを参照してください。

キーボード レイアウト コードの変更 (Sun ターゲット)

この手順は、DCIM-SUSB を使用していて、キーボード レイアウトを別の言語に変更する場合に使用します。

▶ キーボード レイアウト コードを変更するには、以下の手順に従います (DCIM-SUSB のみ)。

1. Sun™ ワークステーション上で［テキスト エディタ］ウィンドウを開きます。

2. Num Lock キーが有効であることを確認した後、キーボードの左の Ctrl キーと Del キーを押すか、[Keyboard] (キーボード) メニューから [Set CIM Keyboard/Mouse options] (CIM キーボード/マウス オプションを設定する) オプションを選択します。

   Caps Lock ライトが点滅して、CIM がレイアウト コード変更モードであることを示します。

   テキスト ウィンドウに、「`Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX)`」と表示されます。

3. 適切なレイアウト コード (たとえば日本語キーボードは *31*) を入力します。Enter キーを押します。
4. デバイスの電源を切った後、再度電源を入れます。DCIM-SUSB がリセット (電源の再投入) されます。
5. 入力した文字が正しく表示されることを確認します。

手順 7: SSL 証明書の作成およびインストール

各 KX III デバイスに固有の SSL 証明書をインストールすることを強くお勧めします。

このセキュリティ ベスト プラクティスにより、Java® 警告メッセージが抑制され、中間者攻撃を受けにくくなります。

また、今後の Java バージョンやブラウザ バージョンから KX III デバイスへのアクセスも阻止されにくくなります。

SSL 証明書の作成およびインストールについては、「*SSL 証明書*『*183*p. 』」を参照してください。

ラック PDU (電源タップ) のコンセントの制御

概要

KX III では、Raritan PX および RPC シリーズのラック PDU (電源タップ) コンセントを制御できます。 これは、D2CIM-PWR を使用して KX III に接続されています。

PX または RPC シリーズをセットアップして KX III に接続すると、そのラック PDU および各コンセントを KX III のユーザ インタフェース (UI) 画面の [Powerstrip] (電源タップ) ページで制御できるようになります。このページを開くには、UI の上端にある [Power] (電源) メニューをクリックします。

[Powerstrip] (電源タップ) ページが開きます。このページには、KX III に接続されており、かつ、ユーザが適切なポートアクセス権限を付与されている、ラック PDU が表示されます。 カスケード接続の場合は、ベース KX III またはカスケード接続 KX III に接続されており、かつ、ユーザが適切なポートアクセス権限を付与されている、ラック PDU が表示されます。

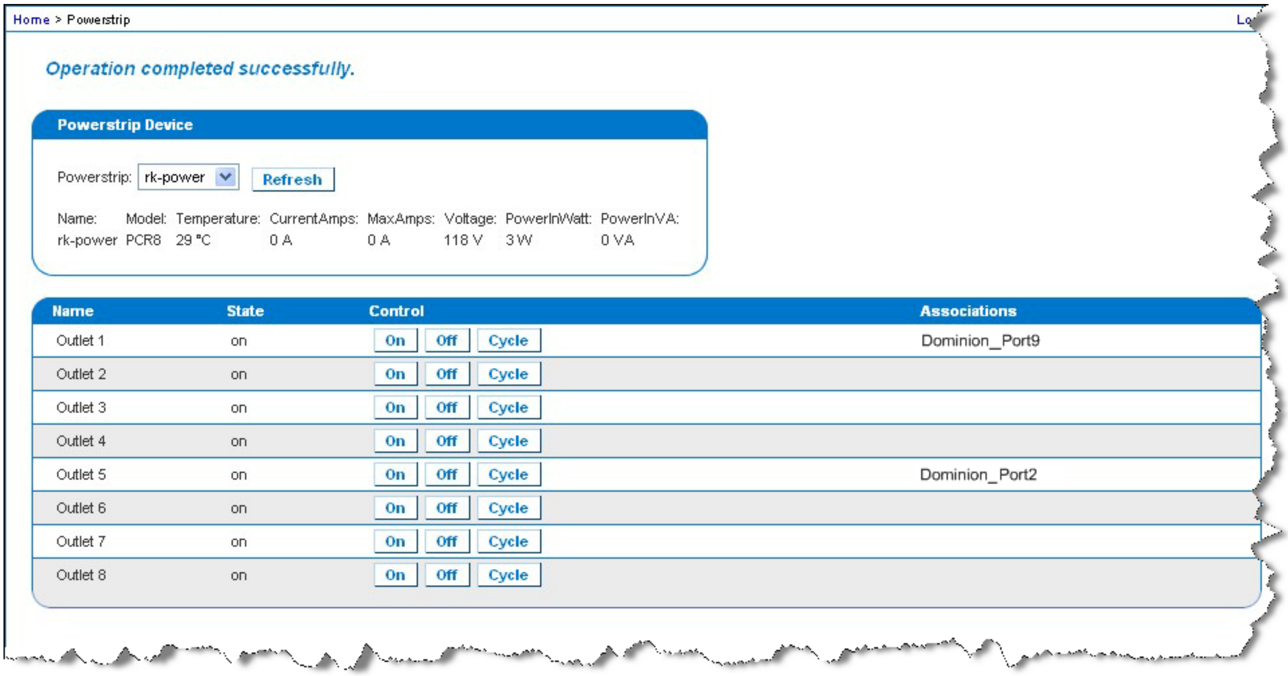
注:PX のセットアップ手順については、『Raritan PX User Guide (Raritan PX ユーザ ガイド)』を参照してください。

[Powerstrip] (電源タップ) ページでは、各コンセントの電源のオン/オフを切り替えること、および、各コンセントの電源を再投入することができます。また、電源タップおよび各コンセントに関する次の情報を表示できます。

- 電源タップに関する情報:
  - [Name] (名前)
  - [Model] (モデル)
  - 温度
  - 電流 (A)
  - 最大電流 (A)
  - 電圧 (V)
  - 電力 (W)
  - 電力 (VA)
- コンセントに関する情報:
  - [Name] (名前): 設定時にコンセントに割り当てた名前。
  - [State] (状態): コンセントの状態 ("on" (オン) または "off" (オフ))。
  - [Control] (制御): コンセントの電源を制御するボタン ([On] (オン)、[Off] (オフ)、および [Cycle] (電源再投入))。

- [Association] (関連ポート): コンセントに関連付けられているポート。

[Powerstrip] (電源タップ) ページを開くと、KX III に接続されている電源タップが [Powerstrip] (電源タップ) ボックスの一覧に表示されます。また、そのボックスに、現在選択されている電源タップに関する情報が表示されます。KX III に接続されている電源タップが 1 台もない場合は、このページの [Powerstrip Device] (電源タップ) セクションに "No powerstrips found" (電源タップが見つかりません) というメッセージが表示されます。



コンセントの電源オン/オフの切り替えまたは電源再投入を行う

▶ コンセントの電源をオンにするには

1. [Power] (電源) メニューをクリックし、[Powerstrip] (電源タップ) ページを開きます。
2. [Powerstrip] (電源タップ) ボックスの一覧で、コンセントの電源をオンにする PX ラック PDU (電源タップ) を選択します。
3. [Refresh] (最新の情報に更新) ボタンをクリックし、各電源制御ボタンを表示します。
4. 電源をオンにするコンセントの横の [On] (オン) をクリックします。
5. 電源オン完了ダイアログ ボックスが開くので、[OK] をクリックして閉じます。コンセントの電源がオンになり、[State] (状態) 列の表示が "on" (オン) になります。

コンセントの電源をオフにするには

1. 電源をオフにするコンセントの横の［Off］（オフ）をクリックします。
2. 電源オフ確認ダイアログ ボックスが開くので、［OK］をクリックして閉じます。
3. 電源オフ完了ダイアログ ボックスが開くので、［OK］をクリックして閉じます。コンセントの電源がオフになり、［State］（状態）列の表示が "off"（オフ）になります。

コンセントの電源を再投入するには

1. 電源を再投入するコンセントの横の［Cycle］（電源再投入）をクリックします。電源再投入確認ダイアログ ボックスが開きます。
2. ［OK］をクリックします。コンセントの電源が再投入されます。電源再投入には数秒かかることがあります。
3. 電源再投入が完了すると、電源再投入完了ダイアログ ボックスが開きます。［OK］をクリックしてこのダイアログ ボックスを閉じます。

USB プロファイル

概要

さまざまな KVM ターゲット サーバと KX III との互換性を高めるために、ラリタンは、幅広いオペレーティング システムおよび BIOS レベルのサーバ実装に対応する USB 設定プロファイルの標準的な選択肢を提供しています。

Generic (デフォルト) USB プロファイルは、展開された KVM ターゲット サーバ設定の大部分のニーズを満たしています。

その他のプロファイルは、一般的に展開される他のサーバ設定 (例: Linux® や Mac OS X®) の特定のニーズを満たすように提供されています。

たとえば BIOS レベルで実行される場合に、ターゲット サーバとの仮想メディア機能の互換性を強化するための、(プラットフォーム名および BIOS のリビジョンによって指定された) プロファイルも多数あります。

USB プロファイルは、KX III リモート コンソールおよびローカル コンソールで、[Device Settings] (デバイス設定)、[Port Configuration] (ポート設定)、[Port] (ポート) ページの順に選択して設定します。

管理者は、ユーザおよびターゲット サーバの設定のニーズに最適な USB プロファイルでポートを設定します。

KVM ターゲット サーバに接続するユーザは、KVM ターゲット サーバの動作状態に応じて、Virtual KVM Client で、これらの設定済みのプロファイルの中から選択します。

たとえば、サーバで Windows® オペレーティング システムが実行されている場合は、Generic プロファイルが最適です。

BIOS メニューの設定の変更または仮想メディア ドライブからの起動を行う場合は、ターゲット サーバ モデルによっては、BIOS プロファイルの方が適している可能性があります。

特定の KVM ターゲットで、ラリタンが提供する標準 USB プロファイルがいずれも適切に機能しない場合は、ラリタン テクニカル サポートにお問い合わせください。

CIM の互換性

USB プロファイルを使用するには、最新のファームウェアを搭載した仮想メディア CIM を使用する必要があります。仮想メディア CIM については、 「*サポートされているコンピュータ インタフェース モジュール (CIM) の仕様* 『*338*p. 』」を参照してください。

使用できる USB プロファイル

現在のリリースの KX III には、次の表に示した USB プロファイルが用意されています。新しいプロファイルは、Raritan が提供する各ファームウェア アップグレードに含まれています。新しいプロファイルが追加されると、それがヘルプに記載されます。

USB プロファイル	説明
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200 BIOS Dell PowerEdge 1950/2950/2970/6950/R200 BIOS には、このプロファイルまたは 'Generic' プロファイルを使用します。 制限: ▪ なし
BIOS Dell OptiPlex ™ キーボードおよびマウスのみ	Dell OptiPlex BIOS アクセス (キーボードおよびマウスのみ) D2CIM-VUSB を使用している場合に、このプロファイルを使用して、Dell OptiPlex BIOS のキーボード機能を持たせます。新しい D2CIM-DVUSB を使用する場合は、'Generic' プロファイルを使用します。 注意: ▪ Optiplex 210L/280/745/GX620 では、仮想メディアをサポートするために、D2CIM-DVUSB を 'Generic' プロファイルで使用する必要があります。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ 仮想メディアはサポートされていません。
BIOS Dell Optiplex 790	BIOS 操作中は、Dell Optiplex 790 にこのプロファイルを使用します。 警告: ▪ USB の列挙は、仮想メディアが接続または切断されるときに開始されます。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ ずれないマウスはサポートされていません。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。

USB プロファイル	説明
BIOS Dell Optiplex 790 キーボードのみ	BIOS 操作中、キーボード マクロを使用するときに、Dell Optiplex 790 にこのプロファイルを使用します。このプロファイルでは、キーボードのみが有効になります。 制限: ▪ マウスは無効になります。 ▪ 仮想 CD-ROM およびディスク ドライブは無効になります。
BIOS DellPowerEdge キーボードおよびマウスのみ	Dell PowerEdge BIOS アクセス（キーボードおよびマウスのみ） D2CIM-VUSB を使用している場合に、このプロファイルを使用して、Dell PowerEdge BIOS のキーボード機能を持たせます。新しい D2CIM-DVUSB を使用する場合は、'Generic' プロファイルを使用します。 注意: ▪ PowerEdge 650/1650/1750/2600/2650 BIOS では、USB CD-ROM およびディスク ドライブは起動可能デバイスとしてはサポートされていません。 ▪ PowerEdge 750/850/860/1850/2850/SC1425 BIOS で仮想メディアをサポートするには、D2CIM-DVUSB を 'Generic' プロファイルで使用する必要があります。 ▪ BIOS で実行している場合は、PowerEdge 1950/2950/2970/6950/R200 に 'BIOS Dell PowerEdge 1950/2950/2970/6950/R200' または 'Generic' プロファイルを使用します。 制限: ▪ USB バス速度はフルスピード（12 MBit/s）に制限されます。 ▪ ずれないマウス（Absolute mouse synchronization™）はサポートされていません。 ▪ 仮想メディアはサポートされていません。
BIOS ASUS P4C800 マザーボード	BIOS にアクセスしたり、Asus P4C800 ベースのシステムで仮想メディアから起動したりするには、このプロファイルを使用します。 制限: ▪ USB バス速度はフルスピード（12 MBit/s）に制限されます。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。

USB プロファイル	説明
BIOS 汎用	BIOS 汎用 このプロファイルは Generic OS プロファイルが BIOS で機能しない場合に使用します。 警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS HP Proliant DL145 PhoenixBIOS では、OS のインストール中に、このプロファイルを使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 HP Compaq DC7100/DC7600 シリーズのデスクトップを仮想メディアから起動するにはこのプロファイルを使用します。 制限: ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS BIOS 操作中は IBM® Thinkcentre Lenovo システム ボード (828841U モデル) にこのプロファイルを使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
アドバンスト マネージメント モジュールを装備した IBM BladeCenter H	D2CIM-VUSB または D2CIM-DVUSB がアドバンスト マネージメント モジュールに接続されている場合に、仮想メディア機能を有効にするには、このプロファイルを使用します。 制限: ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。

USB プロファイル	説明
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 および X61 (仮想メディアから起動) T61 および X61 シリーズのラップトップを仮想メディアから起動するには、このプロファイルを使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。
Generic (汎用)	汎用 USB プロファイルは、オリジナルの KX3 リリースの動作と似ています。このプロファイルは、Windows 2000®、Windows XP®、Windows Vista®、およびそれ以降の Windows に対して使用します。 制限: ▪ なし
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) このプロファイルは、HP Proliant DL360/DL380 G4 シリーズのサーバで HP SmartStart CD を使用して OS をインストールする場合に使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。
HP Proliant DL360/DL380 G4 (Windows® Server 2003 インストール)	HP Proliant DL360/DL380 G4 (Windows Server 2003 インストール) このプロファイルは、HP Proliant DL360/DL380 G4 シリーズのサーバで HP SmartStart CD を使用せずに Windows Server 2003 をインストールする場合に使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。
Linux®	汎用 Linux プロファイル これは、汎用 Linux プロファイルです。Redhat Enterprise Linux、SuSE Linux Enterprise Desktop、および類似のディストリビューションで使用されます。 制限: ▪ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。
BIOS Mac®	BIOS Mac このプロファイルは Mac BIOS に使用します。 制限: ▪ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用するこ

USB プロファイル	説明
	とはできません。 この USB プロファイルを使用する場合、Mac のブート メニューを使用するときのマウス モードについては、「*Mac のブート メニュー使用時のマウス モード* 『*56*p. 』」を参照してください。
MAC OS X® 10.4.9 (以降)	MAC OS X バージョン 10.4.9 (以降) このプロファイルは、最近のバージョンの Mac OS X で導入されたマウス座標のスケーリングを補正します。リモートおよびローカルのマウスの位置がデスクトップの境界の近くで同期しない場合はこれを選択します。 制限: ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
RUBY 工業用メインボード (AwardBIOS)	RUBY 工業用メインボード (AwardBIOS) このプロファイルは、Phoenix/AwardBIOS v6.00PG を使用する RUBY-9715VG2A シリーズの工業用メインボードで使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
Supermicro Mainboard Phoenix (AwardBIOS)	Supermicro メインボード Phoenix (AwardBIOS) このプロファイルは、Phoenix AwardBIOS を使用する Supermicro シリーズのメインボードで使用されます。 制限: ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
Suse 9.2	SuSE Linux 9.2 これは SuSE Linux 9.2 ディストリビューションで使用されます。 制限: ▪ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。 ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。
Troubleshooting 1	トラブルシューティング プロファイル 1 ▪ マス ストレージが優先 ▪ キーボードおよびマウス (タイプ 1) ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。

USB プロファイル	説明
	警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。
Troubleshooting 2	トラブルシューティング プロファイル 2 ▪ キーボードおよびマウス (タイプ 2) 優先 ▪ マス ストレージ ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。 警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。
Troubleshooting 3	トラブルシューティング プロファイル 3 ▪ マス ストレージが優先 ▪ キーボードおよびマウス (タイプ 2) ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。 警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。
仮想メディア CIM でフルスピードを使用	仮想メディア CIM でフルスピードを使用 このプロファイルは、[Full Speed for Virtual Media CIM] (仮想メディア CIM でフルスピードを使用) オプションを選択したオリジナルの KX3 リリースの動作に似ています。高速 USB デバイスを処理できない BIOS に便利です。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。
キーボードおよびマウスの USB でフル スピードを使用	このプロファイルでは、デュアル VM CIM のキーボードおよびマウスの USB インタフェースがフル スピードに設定されます。低速 USB 設定では正しく動作できないデバイスに有効です。 制限: ▪ キーボードおよびマウスの USB インタフェースの USB バス速度は、フル スピード (12 MBit/s) に設定されます。

Mac のブート メニュー使用時のマウス モード

USB プロファイルの使用時に、Mac のブート メニューでマウスを使用するには、ずれないマウス モードが BIOS でサポートされていないので、シングル マウス モードにする必要があります。

▶ **ブート メニューで動作するようにマウスを設定するには、以下の手順に従います。**

1. Mac を再起動し、再起動中に option キーを押してブート メニューを開きます。この時点では、マウスは応答しません。
2. シングル マウス モードを選択します。これで、マウスが応答します。

注:シングル マウス モードでは、マウスの速度が遅くなることがあります。

3. ブート メニューから OS X に戻る場合は、シングル マウス モードを終了し、ずれないマウス モードに切り替えます。

KVM ポート用のプロファイルの選択

KX III には、USB プロファイルのセットが含まれているので、接続先の KVM ターゲット サーバの特性に基づいて KVM ポートを割り当てることができます。KX III リモートまたはローカル コンソールで、[Device Settings] (デバイス設定)、[Port Configuration] (ポート設定)、[Port] (ポート) ページの順に選択し、USB プロファイルを KVM ポートに割り当てています。

特定のターゲットで必要になる可能性が最も高いプロファイルを指定するのは、管理者です。これらのプロファイルは、Virtual KVM Client (VKC) 経由での選択に使用できるようになります。プロファイルを利用できない場合は、[USB Profile] (USB プロファイル) の [Other Profiles] (他のプロファイル) を選択して、使用可能なプロファイルにアクセスできます。

USB プロファイルを KVM ポートに割り当てると、ユーザが KVM ターゲット サーバに接続するときにそれらのプロファイルを使用できるようになります。必要な場合は、Virtual KVM Client (VKC) の [USB Profile] (USB プロファイル) メニューから USB プロファイルを選択できます。

USB プロファイルを KVM ポートに割り当てる方法の詳細は、「*USB プロファイルの設定 ([Port] (ポート) ページ)*『*127*p. 』」を参照してください。

[User Management] (ユーザ管理)

ユーザ グループ

KX III は、アクセスの認可と許可を決定するためにユーザ名とグループ名の内部リストを保持しています。この情報は、暗号化形式で内部に保存されます。認証にはいくつかの方式があり、この方式は「ローカル認証」と呼ばれます。すべてのユーザは認証を受ける必要があります。LDAP/LDAPS または RADIUS 認証を行うように KX III が設定されている場合、その認証が行われた後に、ローカル認証が行われます。

すべての KX III には、3 つのデフォルト ユーザ グループが存在します。これらのグループは削除できません。

ユーザ	説明
[Admin] (管理)	このグループに所属するユーザは、完全な管理者特権を持ちます。元の製品出荷時のデフォルト ユーザはこのグループのメンバーであり、完全なシステム特権を持ちます。さらに、Admin (管理者) ユーザは Admin (管理者) グループのメンバーである必要があります。
Unknown (不明)	LDAP/LDAPS または RADIUS を使用して外部的に認証されるユーザまたはシステムで既知のユーザのデフォルト グループです。外部 LDAP/LDAPS サーバまたは RADIUS サーバによって有効なユーザ グループが識別されなかった場合、Unknown (不明) グループが使用されます。さらに、新規に作成されたユーザは別のグループに割り当てられるまでこのグループに自動的に配置されます。
Individual Group (個別グループ)	個別グループとは、基本的に個人の「グループ」です。つまり、特定のユーザは独自のグループに属し、他の実際のグループには属しません。個別グループは、グループ名の先頭に "@" が付けられているので区別できます。個別グループでは、グループと同じ権限をユーザ アカウントに割り当てることができます。

KX III 内では最大 254 個のユーザ グループを作成できます。 KX III 内では最大 254 個のユーザ グループを作成できます。

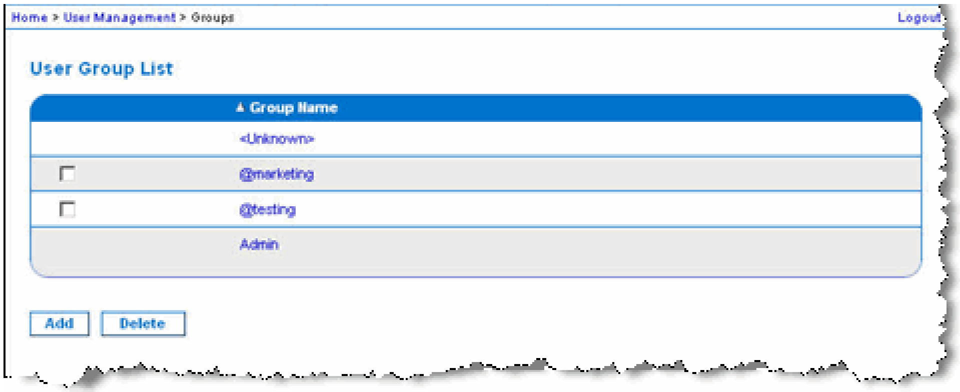
ユーザ グループ リスト

ユーザ グループは、ローカル認証とリモート認証（RADIUS または LDAP/LDAPS）で使用されます。個別のユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。

［ユーザ グループ リスト］ページには、すべてのユーザ グループのリストが表示されます。このリストは、［グループ名］列見出しをクリックすることで、昇順または降順に並べ替えることができます。［ユーザ グループ リスト］ページでは、ユーザ グループを追加、変更、または削除することもできます。

▶ ユーザ グループのリストを表示するには、以下の手順に従います。

- ［ユーザ管理］の［ユーザ グループ リスト］を選択します。［ユーザ グループ リスト］ページが開きます。



ユーザとグループの関係

ユーザはグループに属し、グループには特権が割り当てられています。KX III の各種のユーザをグループに分けることにより、ユーザごとに許可を管理する必要がなくなり、あるグループ内のすべてユーザの許可を一度に管理できるようになるので、時間の節約につながります。

また、特定のユーザをグループに割り当てないようにすることも可能です。その場合は、ユーザを「個別」として分類します。

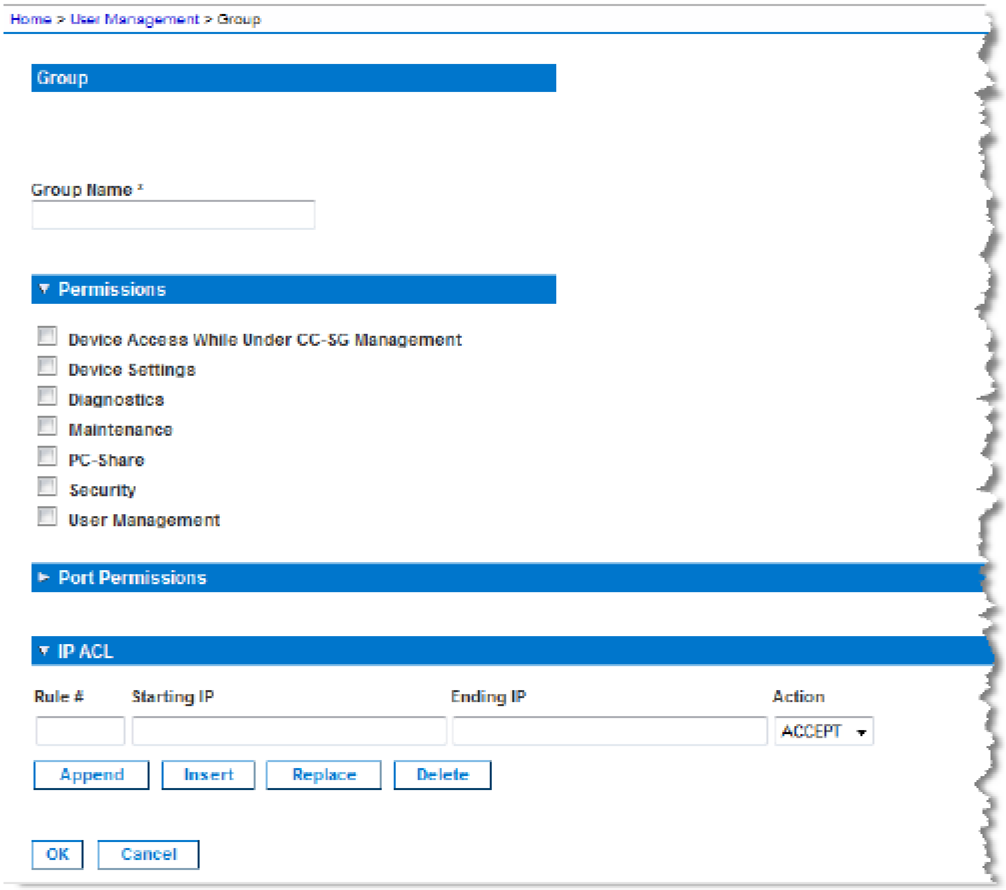
認証が成功すると、デバイスは、グループ情報を使用して、アクセスできるサーバ ポート、デバイスの再起動を許可するかどうかなど、そのユーザの許可を決定します。

新規ユーザ グループの追加

▶ 新規ユーザ グループを追加するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Add New User Group] (新規ユーザ グループの追加) を選択するか、[User Group List] (ユーザ グループ リスト) ページの [Add] (追加) をクリックします。
2. [Group Name] (グループ名) フィールドに、新しいユーザ グループのわかりやすい名前 (最大 64 文字) を入力します。
3. このグループに属するすべてのユーザに対して割り当てる許可の横にあるチェックボックスをオンにします。「許可の設定」を参照してください。
4. このグループに属するユーザがアクセスできるサーバ ポートと、そのアクセスのタイプを指定します。「*ポート権限の設定* 『*62*p. 』」を参照してください。
5. IP ACL を設定します。この機能は、IP アドレスを指定することで、KX III デバイスへのアクセスを制限します。この機能は、特定のグループに属するユーザにのみ適用されます。このデバイスに対するすべてのアクセス試行に適用され、優先される、IP アクセス制御リスト機能とは異なります。「*グループベースの IP ACL (アクセス制御リスト)* 『*63*p. 』」を参照してください。 (オプション)

6. [OK] をクリックします。



許可の設定

許可	説明
[Device Access While Under CC-SG Management] (CC-SG 管理下のデバイス アクセス)	この許可を持つユーザとユーザ グループは、CC-SG のデバイスに対してローカル アクセスが有効になっている場合に IP アドレスを使用して直接 KX III にアクセスできます。デバイスには、 からアクセスできます。 CC-SG の管理下にあるデバイスに直接アクセスすると、KX III でアクセスおよび接続アクティビティがログに記録されます。ユーザ認証は、KX III の認証設定に基づいて実行されます。 *注:管理者ユーザ グループには、この許可がデフォルトで付与されます。*
[Device Settings]	ネットワーク設定、日付/時刻設定、ポート設定

許可	説明
(デバイス設定)	(チャンネル名、電源の関連付け)、イベント管理(SNMP、Syslog)、仮想メディア ファイル サーバのセットアップ。
診断	ネットワーク インタフェース ステータス、ネットワーク統計、ホストへの Ping、ホストへのトレース ルート、KX III 診断
保守	データベースのバックアップと復元、ファームウェアのアップグレード、ファクトリ リセット、再起動
[PC-Share] (PC 共有)	複数のユーザによる同一ターゲットへの同時アクセス カスケード接続構成を使用しており、ベース KX III デバイスから他の複数台のカスケード接続デバイスにアクセスしている場合は、すべてのデバイス間で同じ PC 共有設定を共有する必要があります。カスケード接続の詳細については、「カスケード接続を設定および有効化する」を参照してください。
セキュリティ	SSL 証明書、セキュリティ設定 (VM 共有、PC 共有)、IP ACL
[User Management] (ユーザ管理)	ユーザおよびグループの管理、リモート認証(LDAP/LDAPS/RADIUS)、ログイン設定。 カスケード接続構成にしており、ベース KX III デバイスから他の複数台のカスケード接続デバイスにアクセスしている場合、ユーザ設定、ユーザ グループ設定、およびリモート認証設定をすべてのデバイス間で統一する必要があります。カスケード接続の詳細については、「カスケード接続を設定および有効化する」を参照してください。

ポート権限の設定

それぞれのサーバ ポートに対して、そのグループが持つアクセスのタイプ、仮想メディアへのポート アクセスのタイプ、および電源管理を指定できます。すべての権限についてデフォルト設定はすべて [Deny] (拒否) になっていることに注意してください。

ポート アクセス	
オプション	**説明**
[Deny] (拒否)	アクセスを完全に拒否します。
[View] (表示)	接続先のターゲット サーバのビデオを表示します (操作はできません)。
[Control] (制御)	接続先のターゲット サーバを制御します。VM および電源管理アクセスも付与される場合は、[Control] (制御) を割り当てる必要があります。 追加された KVM スイッチをユーザ グループ内のすべてのユーザが表示できるようにするためには、各ユーザに [Control] (制御) アクセスが付与されている必要があります。この権限を持たないユーザには、KVM スイッチが後で追加されても、スイッチは表示されません。 アクティブになるコントロールに関連する音声またはスマート カードに対する [Control] (制御) アクセスの付与が必要です。

VM アクセス	
オプション	**説明**
[Deny] (拒否)	ポートに対して仮想メディア許可はすべて拒否されます。
[Read-Only] (読み取り専用)	仮想メディア アクセスは、読み取りアクセスのみに制限されます。
[Read-Write] (読み取り/書き込み可能)	仮想メディアに対する完全なアクセス (読み取り、書き込み) が許可されます。

VM アクセス 電源管理アクセス オプション	説明
[Deny] (拒否)	ターゲット サーバに対する電源管理を拒否します。
[Access] (アクセス)	ターゲット サーバでの電源管理を完全に許可します。

ブレード シャーシの場合、ポート アクセス権限によって、そのブレード シャーシに設定されている URL へのアクセスを制御します。オプションは、[Deny] (拒否) または [Control] (制御) です。また、シャーシ内の各ブレードには、固有の独立ポート権限設定があります。

ティアー接続構成にしており、ベース KX III デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、カスケード接続デバイスでは個別のポート制御レベルが適用されます。カスケード接続の詳細については、「カスケード接続を設定および有効化する」を参照してください。

個別グループの許可の設定

▶ 個別ユーザ グループに許可を設定するには、以下の手順に従います。

1. グループ リストから目的のグループを探します。個別グループは、グループ名の先頭に @ が付けられているので区別できます。
2. グループ名をクリックします。[Group] (グループ) ページが開きます。
3. 適切な許可を選択します。
4. [OK] をクリックします。

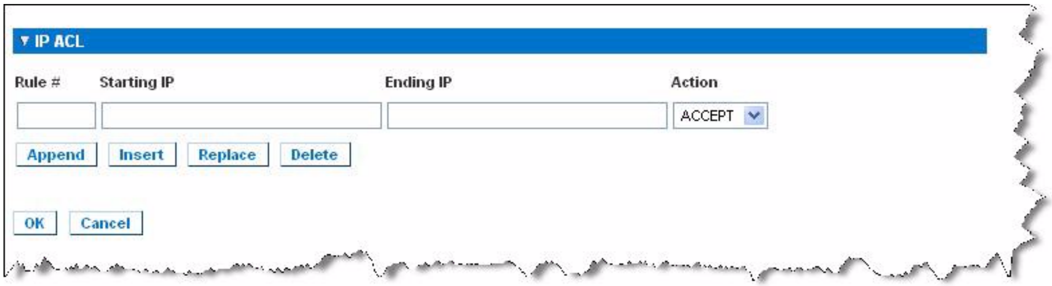
*グループベースの **IP ACL** (アクセス制御リスト)*

重要: グループベースの IP アクセス制御を使用する場合は注意が必要です。アクセスが拒否されている IP アドレスの範囲に自分の IP アドレスが含まれている場合、KX III がロックアウトされてしまいます。

この機能は、選択したグループに含まれるユーザによる KX III デバイスへのアクセスを特定の IP アドレスに制限します。この機能は、デバイスへのすべてのアクセス試行に適用される (および最初に処理され、優先される) IP アクセス制御リスト機能とは異なり、特定のグループに属するユーザにのみ適用されます。

重要: KX III ローカル ポートでは、IP アドレス 127.0.0.1 が使用され、ブロックはできません。

グループレベルで IP アクセス制御ルールの追加、挿入、置換、削除を行うには、[Group] (グループ) ページの [IP ACL] (IP ACL) セクションを使用します。



ルールを一覧の末尾に追加するには

1. [Starting IP] (開始 IP) フィールドに、開始 IP アドレスを入力します。
2. [Ending IP] (終了 IP) フィールドに、終了 IP アドレスを入力します。
3. 利用可能なオプションからアクションを選択します。
   - [Accept] (承諾) – その IP アドレスによる KX III デバイスへのアクセスが許可されます。
   - [Drop] (拒否) – その IP アドレスによる KX III デバイスへのアクセスが拒否されます。
4. [Append] (追加) をクリックします。そのルールがルール一覧の末尾に追加されます。入力する各ルールについて、手順 1 ～ 4 を繰り返します。

ルールを一覧の途中に挿入するには

1. ルール番号 (#) を入力します。[Insert] (挿入) コマンドを使用する際にルール番号が必要です。
2. [Starting IP] (開始 IP) フィールドと [Ending IP] (終了 IP) フィールドに IP アドレスを入力します。
3. [Action] (アクション) ドロップダウン リストからアクションを選択します。
4. [Insert] (挿入) をクリックします。入力したルール番号が既存のルール番号と同じである場合は、新しいルールは既存のルールの上に挿入され、リスト内のすべてのルールが下に下がります。

ルールの内容を置換するには

1. 置き換えるルール番号を指定します。
2. [Starting IP] (開始 IP) フィールドと [Ending IP] (終了 IP) フィールドに IP アドレスを入力します。
3. ドロップダウン リストからアクションを選択します。

4. [Replace] (置換) をクリックします。同じルール番号を持つ元のルールが新しいルールに置き換わります。

ルールを削除するには

1. 削除するルール番号を指定します。
2. [Delete] (削除) をクリックします。
3. 削除を確認するプロンプトが表示されたら、[OK] をクリックします。

重要: ACL のルールは、リスト表示されている順に評価されます。たとえばこの例において、2 つの ACL ルールの順番が逆になると、Dominion は通信を全く受けることができなくなります。

```
Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT

Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP
```

ヒント: ルール番号を使用すると、各ルールを作成する順序を気にせずに済みます。

既存のユーザ グループの変更

注:Admin (管理者) グループに対しては、すべての許可が有効になっており、変更はできません。

既存のユーザ グループを変更するには、以下の手順に従います。

1. [Group] (グループ) ページで、適切なフィールドを変更し、適切な許可を設定します。
2. グループに対する許可を設定します。このグループに属するすべてのユーザに対して割り当てる許可の左にあるチェックボックスをオンにします。「許可の設定」を参照してください。
3. [Port Permissions] (ポート権限) を設定します。このグループに属するユーザがアクセスできるサーバ ポート (およびアクセスのタイプ) を指定します。「***ポート権限の設定***『*62*p. 』」を参照してください。
4. IP ACL を設定します (オプション)。この機能は、IP アドレスを指定することで、KX III デバイスへのアクセスを制限します。「***グループベースの IP ACL (アクセス制御リスト)***『*63*p. 』」を参照してください。
5. [OK] (OK) をクリックします。

ユーザ グループを削除するには、以下の手順に従います。

重要: ユーザを含むグループを削除すると、そのユーザは <Unknown (不明)> ユーザ グループに自動的に割り当てられます。

ヒント: 特定のグループに属しているユーザを調べるには、ユーザ グループ別にユーザ リストを並べ替えます。

1. リストのグループ名の左にあるチェックボックスをオンにして、目的のグループを選択します。
2. [Delete] (削除) をクリックします。
3. 削除を確認するプロンプトが表示されたら、[OK] をクリックします。

ユーザ

ユーザが KX III にアクセスするには、ユーザ名とパスワードを付与されている必要があります。この情報は、KX III にアクセスしようとしているユーザを認証するために使用されます。

各ユーザ グループに対して最大 254 ユーザを作成できます。

ティアー接続構成にしており、ベース KX III デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、ユーザは、ベース デバイスにアクセスする許可、および、(必要に応じて) 個々のカスケード接続デバイスにアクセスする許可を必要とします。

ユーザがベース デバイスにログオンすると、各カスケード接続デバイスが照会され、ユーザは、アクセス許可を得ている各ターゲット サーバにアクセスできます。 ティアー接続の詳細については、「ティアー接続を設定および有効化する」を参照してください。

新規ユーザの追加

KX III ユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。「**新規ユーザ グループの追加**」を参照してください。

[User] (ユーザ) ページでは、新規ユーザの追加、ユーザ情報の変更、無効化されているユーザの再有効化を行うことができます。

注: ユーザがログインに失敗した回数が [Security Settings] (セキュリティ設定) ページで設定されているログイン失敗の最大許容回数を超えた場合、そのユーザ名は無効化されます。「**セキュリティの設定**『168p. 』」*を参照してください。*

▶ **新規ユーザを追加するには、以下の手順に従います。**

1. [User Management] (ユーザ管理) の [Add New User] (新規ユーザの追加) を選択するか、[User List] (ユーザ リスト) ページで [Add] (追加) をクリックします。
2. [Username] (ユーザ名) フィールドに、一意のユーザ名 (最大 16 文字) を入力します。

3. [Full Name] (フル ネーム) フィールドに、ユーザのフル ネーム（最大 64 文字）を入力します。
4. [Password] (パスワード) フィールドにパスワードを入力し、[Confirm Password] (パスワードの確認) フィールドにパスワード（最大 64 文字）を再入力します。
5. [User Group] (ユーザ グループ) ドロップダウン リストからグループを選択します。

   このユーザを既存のユーザ グループに関連付けたくない場合は、ドロップダウン リストから [Individual Group] (個別グループ) を選択します。個別グループの許可についての詳細は、「***個別グループの許可の設定*** 『*63*p. 』」を参照してください。
6. 新規ユーザを有効にするには、[アクティブ] チェックボックスをオンのままにします。[OK] をクリックします。

KX III ユーザ リストの表示

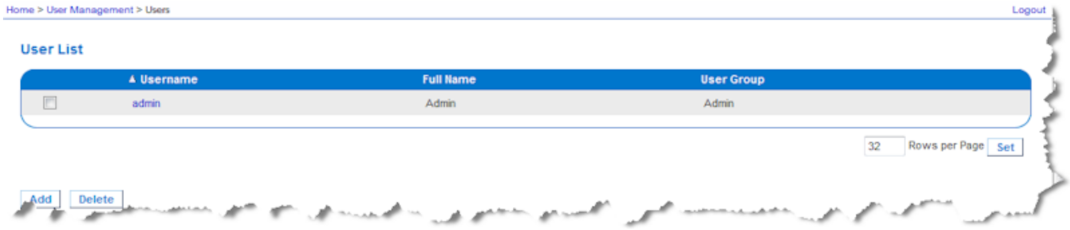
[User List] (ユーザ リスト) ページには、すべてのユーザについて、ユーザ名、フル ネーム、およびユーザ グループが表示されます。このリストは、任意の列名をクリックすることで並べ替えることができます。[User List] (ユーザ リスト) ページでは、ユーザを追加、変更、または削除できます。

ユーザ管理権限を持つ KX III ユーザは、必要に応じてユーザをポートから切断するか、ログオフ（強制ログオフ）することができます。「***ポートからのユーザの切断*** 『*68*p. 』」および「***KX III からのユーザのログオフ（強制ログオフ）*** 『*69*p. 』」をそれぞれ参照してください。

各ユーザの接続先ターゲット ポートを表示するには、「***ポート別のユーザの表示*** 『*68*p. 』」を参照してください。

▶ ユーザ リストを表示するには、以下の手順に従います。

- [User Management] (ユーザ管理) の [User List] (ユーザ リスト) を選択します。[User List] (ユーザ リスト) ページが開きます。



ポート別のユーザの表示

[User By Ports] (ポート別ユーザ) ページには、認証済みのすべてのローカル ユーザとリモート ユーザおよび各ユーザの接続先のポートが表示されます。ポートへの永続的な接続のみが表示されます。ポートのスキャン時にアクセスされているポートは表示されません。

同じユーザが複数のクライアントからログオンしている場合は、接続ごとにユーザ名がページに表示されます。たとえば、ユーザが 2 つの異なるクライアントからログオンしている場合、そのユーザ名が 2 回表示されます。

このページには、次のユーザ情報およびポート情報が表示されます。

- [Port Number] (ポート番号) – ユーザの接続先ポートに割り当てられているポート番号
- [Port Name] (ポート名) – ユーザの接続先ポートに割り当てられているポート名

注:ユーザがターゲットに接続されていない場合は、[Port Name] (ポート名) の下に [Local Console] (ローカル コンソール) または [Remote Console] (リモート コンソール) が表示されます。

- [Username] (ユーザ名) – ユーザ ログインやターゲット接続用のユーザ名
- [Access From] (アクセス元) – KX III にアクセスしているクライアント PC の IP アドレス
- [Status] (ステータス) – 接続の現在のステータス (アクティブまたは非アクティブ)

▶ **ポート別にユーザを表示するには、以下の手順に従います。**

- [User Management] (ユーザ管理) の [Users by Port] (ポート別ユーザ) を選択します。[Users by Port] (ポート別ユーザ) ページが開きます。

ポートからのユーザの切断

ユーザの切断では、ユーザは KX III をログオフしなくてもターゲット ポートから切断されます。

注: ユーザのログオフでは、ユーザはターゲット ポートから切断され、KX III からログオフされます。ユーザの強制ログオフについては、「**KX III からのユーザのログオフ (強制ログオフ)**『69p. 』」*を参照してください。*

▶ **ユーザをポートから切断するには、以下の手順に従います。**

1. [User Management] (ユーザ管理) の [Users by Port] (ポート別ユーザ) を選択します。[Users by Port] (ポート別ユーザ) ページが開きます。

2. ターゲットから切断するユーザの名前の横にあるチェックボックスをオンにします。
3. [Disconnect User from Port] (ポートからのユーザの切断) をクリックします。
4. 確認メッセージに対して [OK] をクリックすると、ユーザがポートから切断されます。
5. ユーザがポートから断されたことを示す確認メッセージが表示されます。

KX III からのユーザのログオフ (強制ログオフ)

管理者である場合は、KX III にログオンしているユーザのうち、認証されているユーザをログオフすることができます。また、ユーザをポートレベルでポートから切断することもできます。「*ポートからのユーザの切断* 『*68*p. 』」を参照してください。

▶ ユーザを KX III からログオフするには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Users by Port] (ポート別ユーザ) を選択します。[Users by Port] (ポート別ユーザ) ページが開きます。
2. ターゲットから切断するユーザの名前の横にあるチェックボックスをオンにします。
3. [Force User Logoff] (ユーザの強制ログオフ) をクリックします。
4. [Logoff User] (ユーザのログオフ) の確認メッセージに対して [OK] をクリックします。

既存のユーザ グループの変更

▶ 既存のユーザを変更するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [User List] (ユーザ リスト) を選択して、[User List] (ユーザ リスト) ページを開きます。
2. [User List] (ユーザ リスト) ページのリストから目的のユーザを探します。
3. ユーザ名をクリックします。[User] (ユーザ) ページが開きます。
4. [User] (ユーザ) ページで、目的のフィールドを変更します [User] (ユーザ) ページにアクセスする方法についての詳細は、「*新規ユーザの追加* 『*66*p. 』」を参照してください。
5. ユーザを削除するには、[Delete] (削除) をクリックします。削除してよいかどうかを確認するダイアログ ボックスが開きます。
6. [OK] (OK) をクリックします。

[Authentication Settings] (認証設定)

認証とは、ユーザが本物であることを確認するプロセスです。ユーザが認証されると、ユーザの属するグループに基づいて、システムおよびポートに対する許可が決定されます。ユーザに割り当てられた特権により、どのようなタイプのアクセスが許可されるかが決まります。これを「認可」と呼びます。

KX III がリモート認証用に構成されている場合、外部認証サーバは主に認証を目的として使用され、認可用には使用されません。

ティアー接続構成にしており、ベース KX III デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、ベース デバイスと各ティアー接続デバイスで同じ認証設定を使用する必要があります。

[Authentication Settings] (認証設定) ページでは、KX III へのアクセスに使用する認証の種類を設定できます。

注: リモート認証 (LDAP/LDAPS または RADIUS) を選択すると、ユーザが見つからない場合はローカル認証データベースも確認されます。

▶ **認証を設定するには、以下の手順に従います。**

1. [ユーザ管理] の [認証設定] を選択します。[認証設定] ページが開きます。
2. 使用する認証プロトコルのオプションを選択します ([ローカル認証]、[LDAP/LDAPS]、または [RADIUS])。[LDAP] オプションを選択した場合、LDAP に関連するフィールドが有効になります。[RADIUS] オプションを選択した場合、RADIUS に関連するフィールドが有効になります。
3. [ローカル認証] を選択した場合は、手順 6 に進みます。
4. [LDAP/LDAPS] を選択した場合は、「LDAP/LDAPS リモート認証の実装」を参考にして、[認証設定] ページの [LDAP] セクションの各フィールドを指定してください。
5. [RADIUS] を選択した場合は、「RADIUS リモート認証の実装」を参考にして、[認証設定] ページの [RADIUS] セクションの各フィールドを指定してください。
6. [OK] をクリックして保存します。

▶ **工場出荷時のデフォルトに戻すには、以下の手順に従います。**

- [デフォルトに戻す] をクリックします。

LDAP/LDAPS リモート認証の実装

Lightweight Directory Access Protocol (ライトウェイト ディレクトリ アクセス プロトコル: LDAP/LDAPS) は、TCP/IP 上で動作するディレクトリ サービスを照会および変更するためのネットワーキング プロトコルです。クライアントは、LDAP/LDAPS サーバ (デフォルトの TCP ポートは 389) に接続して、LDAP セッションを開始します。次に、クライアントは、オペレーション要求をサーバに送信します。サーバは、この要求に対して応答を返します。

メモ: Microsoft Active Directory は、LDAP/LDAPS 認証サーバとしてネイティブに機能します。

▶ LDAP 認証プロトコルを使用するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Authentication Settings] (認証設定) をクリックして、[Authentication Settings] (認証設定) をページを開きます。
2. [LDAP] (LDAP) ラジオ ボタンを選択して、ページの [LDAP] (LDAP) セクションを有効にします。
3.

アイコンをクリックして、ページの [LDAP] (LDAP) セクションを展開します。

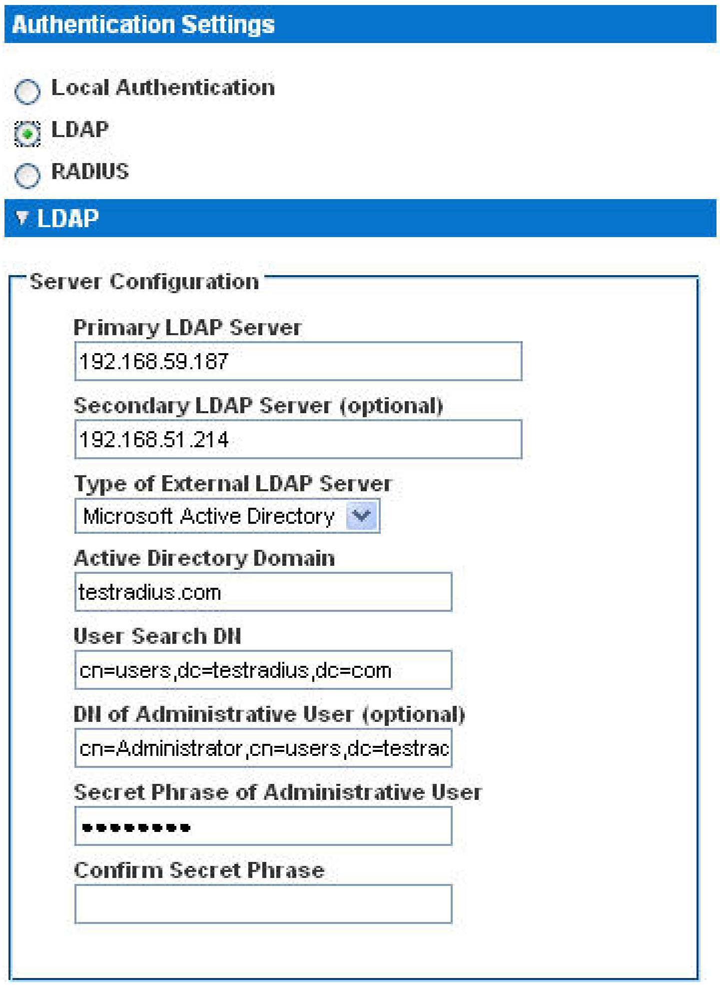
   サーバの設定

4. [Primary LDAP Server] (プライマリ LDAP サーバ) フィールドに、LDAP/LDAPS リモート認証サーバの IP アドレスまたは DNS 名を入力します (最大 256 文字)。[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスをオンにし、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスをオンにした場合は、LDAP サーバ証明書の CN に一致する DNS 名を使用する必要があります。
5. [Secondary LDAP Server] (セカンダリ LDAP サーバ) フィールドに、バックアップ LDAP/LDAPS サーバの IP アドレスまたは DNS 名を入力します (最大 256 文字)。[Enable Secure LDAP] (セキュア LDAP を有効にする) オプションをオンにした場合は、DNS 名を使用する必要があります。残りのフィールドについては、[Primary LDAP Server] (プライマリ LDAP サーバ) フィールドの場合と同じ設定を使用します。**(オプション)**
6. [Type of External LDAP Server] (外部 LDAP サーバの種類)。
7. 外部 LDAP/LDAPS サーバを選択します。使用可能なオプションを選択します。
   - [Generic LDAP Server] (一般的な LDAP サーバ)。
   - [Microsoft Active Directory]。Active Directory は、Windows 環境向けの Microsoft による LDAP/LDAPS ディレクトリ サービスの実装です。

8. Microsoft Active Directory を選択した場合は、Active Directory ドメインの名前を入力します。たとえば、*acme.com* などです。特定のドメインの名前については、Active Directive 管理者にお問い合わせください。
9. [User Search DN] (ユーザ検索 DN) フィールドに、LDAP データベース内でユーザ情報の検索を開始する場所の識別名を入力します。最大 64 文字まで使用できます。たとえば、`cn=Users,dc=raritan,dc=com` というベース検索値を設定します。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。
10. [DN of administrative User] (管理者ユーザの DN) フィールドに管理者ユーザの識別名を入力します (最大 64 文字)。このフィールドは、LDAP サーバで管理者に管理者ユーザの役割を使用したユーザ情報の検索を許可している場合にのみ入力します。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。たとえば、管理者ユーザの DN として、以下のように設定します。

    `cn=Administrator,cn=Users,dc=testradius,dc=com`(オプション)

11. 管理者ユーザの識別名を入力した場合は、管理者ユーザの DN をリモート認証サーバに対して認証するために使用するパスワードを入力する必要があります。[Secret Phrase] (秘密フレーズ) フィールドにパスワードを入力し、[Confirm Secret Phrase] (秘密フレーズの確認) フィールドにパスワードを再入力します (最大 128 文字)。



LDAP/LDAP Secure

12. SSL を使用する場合は、[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスをオンにします。これにより、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスがオンになります。Secure Sockets Layer (SSL) は、KX III が LDAP/LDAPS サーバと安全に通信できるようにする暗号プロトコルです。
13. [Port] (ポート) のデフォルトは 389 です。標準 LDAP TCP ポートを使用するか、または別のポートを指定します。

14. [Secure LDAP Port]（セキュア LDAP ポート）のデフォルトは 636 です。デフォルトのポートを使用するか、または別のポートを指定します。このフィールドは、[Enable Secure LDAP]（セキュア LDAP を有効にする）チェックボックスがオンのときにのみ使用します。
15. 前にアップロードしたルート CA 証明書ファイルを使用してサーバから提供された証明書を検証するには、[Enable LDAPS Server Certificate Validation]（LDAPS サーバ証明書の検証を有効にする）チェックボックスをオンにします。前にアップロードしたルート CA 証明書ファイルを使用しない場合は、このチェックボックスをオフのままにします。この機能を無効にすることは、不明な証明機関によって署名された証明書を受け取ることと同じです。このチェックボックスは、[Enable Secure LDAP]（セキュア LDAP を有効にする）チェックボックスがオンのときにのみ使用できます。

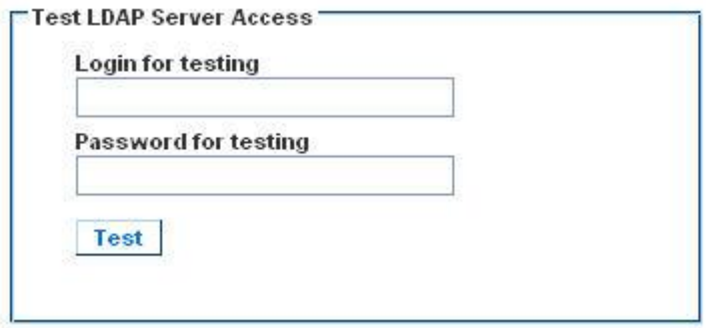
注: 検証にルート CA 証明書を使用し、さらに [Enable LDAPS Server Certificate Validation]（LDAPS サーバ証明書の検証を有効にする）チェックボックスをオンにする場合は、サーバ ホスト名がサーバ証明書に記載された共通名と一致する必要があります。

16. 必要な場合は、ルート CA 証明書のファイルをアップロードします。このフィールドは、[セキュア LDAP を有効にする] チェックボックスがオンのときに有効になります。LDAP/LDAPS サーバ用の Base64 エンコードの X-509 形式の CA 証明書ファイルについては、担当の認証サーバ管理者に問い合わせてください。[参照] を使用して証明書ファイルを選択します。LDAP/LDAPS サーバの証明書を新しい証明書に置き換える場合は、新しい証明書を有効にするために KX III を再起動する必要があります。

LDAP サーバ アクセスのテスト

17. LDAP サーバおよび KX III をリモート認証用に正しく構成するために複雑な設定が必要になることがあるので、KX III には、[Authentication Settings] (認証設定) ページから LDAP の設定をテストする機能が用意されています。LDAP の設定をテストするには、[Login for testing] (テスト用ログイン) フィールドと [Password for testing] (テスト用パスワード) フィールドにそれぞれログイン名とパスワードを入力します。これは、KX III にアクセスするときに入力したユーザ名とパスワードです。LDAP サーバはこれを使用してユーザを認証します。[Test] (テスト) をクリックします。

    テストが完了すると、テストが成功したことを知らせるメッセージが表示されます。テストが失敗した場合は、詳細なエラー メッセージが表示されます。成功したことが表示されるか、または失敗した場合は詳細なエラー メッセージが表示されます。成功時には、リモート LDAP サーバから取得されたテスト ユーザのグループ情報も表示されることがあります。



ユーザ グループ情報を Active Directory サーバから返す

KX III では Active Directory® (AD) を使用したユーザ認証がサポートされているので、ユーザを KX III でローカルに定義する必要はありません。これにより、Active Directory のユーザ アカウントとパスワードは、AD サーバ上に排他的に維持されます。認可と AD ユーザ特権は、標準の KX III ポリシー、および AD ユーザ グループにローカルに適用されるユーザ グループ特権によって制御および管理されます。

重要: Raritan, Inc. の既存のお客様がすでに AD スキーマを変更して Active Directory サーバを設定している場合、KX III はこの設定をサポートします。この場合、以下に示す手順を実行する必要はありません。AD LDAP/LDAPS スキーマを更新する方法の詳細については、「LDAP スキーマの更新」を参照してください。

▶ **KX III で AD サーバを有効にするには、以下の手順に従います。**

1. KX III を使用して、特殊なグループを作成し、適切な許可および特権をグループに割り当てます。たとえば、KVM_Admin や KVM_Operator というグループを作成します。

2. Active Directory サーバで、前の手順で作成したのと同じグループ名を持つ新しいグループを作成します。
3. AD サーバ上で、手順 2 で作成したグループに KX III ユーザを割り当てます。
4. KX III で、AD サーバを有効にし、適切に設定します。「*LDAP/LDAPS リモート認証の実装* 『*71*p. 』」を参照してください。

重要な注記:

- グループ名では大文字と小文字が区別されます。
- KX III には、[管理者] と [<不明>] のデフォルト グループが用意されています。これらのグループを変更したり削除したりすることはできません。Active Directory サーバでこれらと同じグループ名が使用されていないことを確認してください。
- Active Directory サーバから返されたグループ情報が KX III のグループ設定と一致しない場合、正常に認証されたユーザに対して自動的に [<不明>] グループが割り当てられます。
- ダイヤルバック番号を使用する場合は、次の文字列を入力する必要があります。大文字と小文字は区別されます。*msRADIUSCallbackNumber*
- Microsoft からの推奨に基づいて、ドメイン ローカル グループではなく、ユーザ アカウントを含むグローバル グループを使用する必要があります。

RADIUS リモート認証の実装

Remote Authentication Dial-in User Service (RADIUS) は、ネットワーク アクセス アプリケーションのための AAA (認証 (authentication)、認可 (authorization)、アカウンティング (accounting)) プロトコルです。

▶ RADIUS 認証プロトコルを使用するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Authentication Settings] (認証設定) をクリックして、[Authentication Settings] (認証設定) をページを開きます。
2. [RADIUS] (RADIUS) ラジオ ボタンをクリックして、ページの [RADIUS] (RADIUS) セクションを有効にします。
3.

アイコンをクリックして、ページの [RADIUS] (RADIUS) セクションを展開します。
4. [Primary Radius Server] (プライマリ Radius サーバ) フィールドおよび [Secondary Radius Server] (セカンダリ Radius サーバ) フィールドに、プライマリ認証サーバの IP アドレスおよびオプションでセカンダリ認証サーバの IP アドレスを入力します (最大 256 文字)。
5. [Shared Secret] (共有の秘密) フィールドに、認証に使用するサーバの秘密フレーズを入力します (最大 128 文字)。

共有の秘密とは、KX III と RADIUS サーバとの間で安全に通信を行うために両者で共有される文字列です。これは、基本的にはパスワードです。

6. [Authentication Port] (認証ポート) のデフォルトは 1812 ですが、必要に応じて変更できます。
7. [Accounting Port] (アカウンティング ポート) のデフォルトは 1813 ですが、必要に応じて変更できます。
8. [Timeout] (タイムアウト) は秒単位で記録され、デフォルトは 1 秒ですが、必要に応じて変更できます。

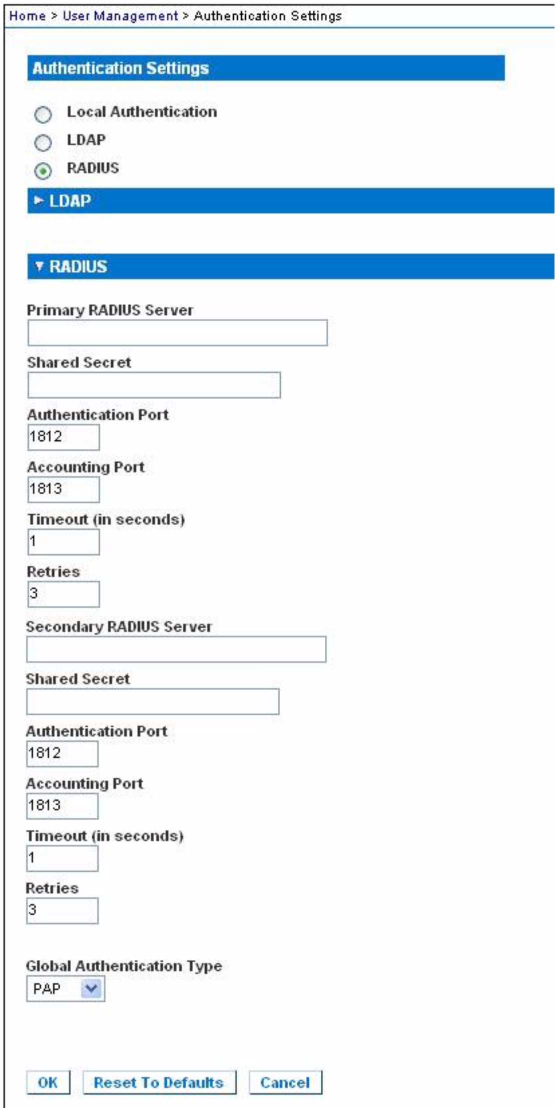
   このタイムアウトは、KX III が次の認証要求を送信する前に RADIUS サーバからの応答を待つ時間です。

9. デフォルトの再試行回数は 3 回です。

   これは、KX III が RADIUS サーバに対して認証要求を送信する回数です。

10. ドロップダウン リストのオプションから、適切な [Global Authentication Type] (グローバル認証タイプ) を選択します。
    - [PAP] (PAP) – PAP の場合、パスワードは平文 (ひらぶん) – 暗号化されないテキストとして送信されます。PAP は対話型ではありません。サーバがログイン プロンプトを送信してその応答を待つ方式ではなく、接続が確立された時点でユーザ名とパスワードが 1 つのデータ パッケージとして送信されます。

- [CHAP] (CHAP) – CHAP の場合、サーバはいつでも認証を要求できます。CHAP は、PAP よりも高いセキュリティを実現します。



RADIUS 認証用の Cisco ACS 5.x

Cisco ACS 5.x サーバを使用している場合は、KX III に RADIUS 認証を設定した後に、Cisco ACS 5.x サーバで以下の手順を完了する必要があります。

注: 以下の手順には、各ページへのアクセスに使用される Cisco のメニューおよびメニュー項目が含まれます。各手順の最新情報とその実行の詳細については、Cisco のマニュアルを参照してください。

- AAA クライアントとしての KX III の追加 (**必須**) - [Network Resources] (ネットワーク リソース)、[Network Device Group] (ネットワーク デバイス グループ)、[Network Device and AAA Clients] (ネットワーク デバイスと AAA クライアント) の順に選択
- ユーザの追加/編集 (**必須**) - [Network Resources] (ネットワーク リソース)、[Users and Identity Stores] (ユーザ ストアと ID ストア)、[Internal Identity Stores] (内部 ID ストア)、[Users] (ユーザ) の順に選択
- CHAP プロトコルを有効にするデフォルト ネットワーク アクセスの設定 (**オプション**) - [Policies] (ポリシー)、[Access Services] (アクセス サービス)、[Default Network Access] (デフォルト ネットワーク アクセス) の順に選択
- アクセスを制御する認可ポリシー ルールの作成 (**必須**) - [Policy Elements] (ポリシー要素)、[Authorization and Permissions] (認可と許可)、[Network Access] (ネットワーク アクセス)、[Authorization Profiles] (認可プロファイル) の順に選択
  - [Dictionary Type] (ディクショナリ タイプ): RADIUS-IETF
  - [RADIUS Attribute] (RADIUS 属性): Filter-ID
  - [Attribute Type] (属性タイプ): String
  - [Attribute Value] (属性値): Raritan:G{KVM_Admin} (KVM_Admin は Dominion KVM Switch でローカルに作成されたグループ名)。大文字と小文字が区別されます。
- セッション状況 (日時) の設定 (**必須**) - [Policy Elements] (ポリシー要素)、[Session Conditions] (セッション状況)、[Date and Time] (日時) の順に選択
- ネットワーク アクセス認可ポリシーの設定/作成 (**必須**) - [Access Policies] (アクセス ポリシー)、[Access Services] (アクセス サービス)、[Default Network Access] (デフォルト ネットワーク アクセス)、[Authorization] (認可) の順に選択

ユーザ グループ情報を RADIUS 経由で返す

RADIUS 認証の試行が成功したら、KX III は、ユーザのグループの許可に基づいて、そのユーザの許可を決定します。

リモート RADIUS サーバは、RADIUS FILTER-ID として実装された属性を返すことによって、これらのユーザ グループ名を提供できます。FILTER-ID は、Raritan:G{*GROUP_NAME*} という形式となります。*GROUP_NAME* は、ユーザが属するグループの名前を示す文字列です。

```
Raritan:G{GROUP_NAME}:D{Dial Back Number}
```

GROUP_NAME は、ユーザが属するグループの名前を示す文字列です。Dial Back Number は、ユーザ アカウントに関連付けられている番号で、KX III モデムがユーザ アカウントへのダイヤルバックに使用します。

RADIUS 通信交換仕様

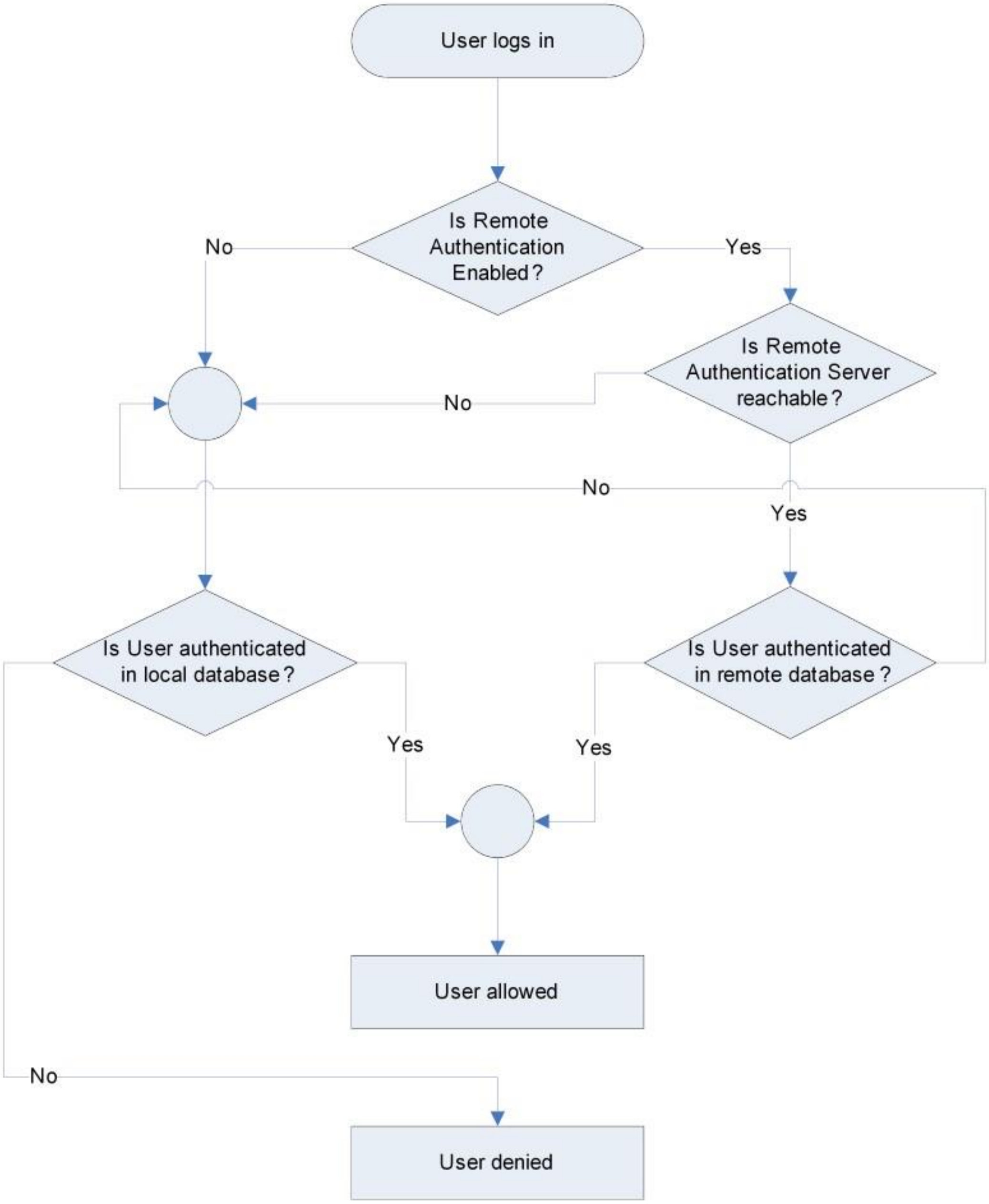
KX III は、以下の RADIUS 属性を RADIUS サーバに送信します。

属性	データ
ログイン	
Access-Request(1)	
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-IP-Address (4)	KX III の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
User-Password(2):	暗号化されたパスワード
Accounting-Request(4)	
Acct-Status (40)	Start(1) - アカウンティングを開始する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	KX III の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
ログアウト	
Accounting-Request(4)	

属性	データ
Acct-Status (40)	Stop(2) - アカウンティングを停止する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	KX III の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID

ユーザ認証プロセス

リモート認証は、その後のフローチャートに指定されたプロセスに従います。

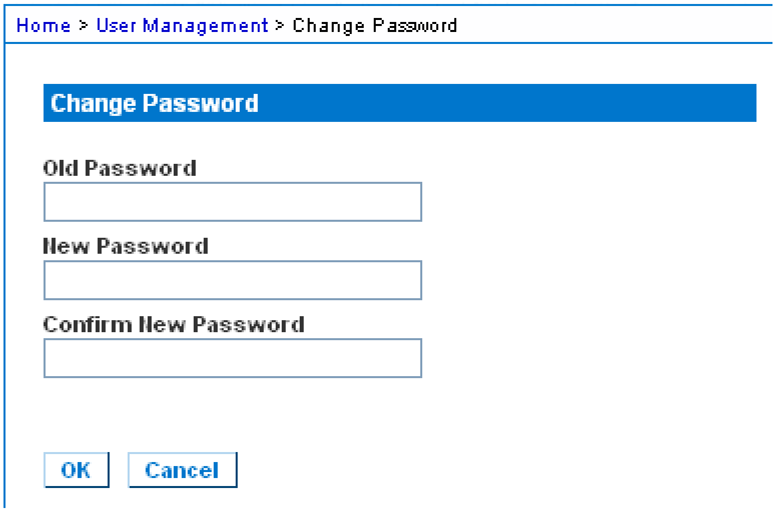


パスワードの変更

▶ KX III パスワードを変更するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Change Password] (パスワードの変更) を選択します。[Change Password] (パスワードの変更) ページが開きます。
2. [Old Password] (旧パスワード) フィールドに現在のパスワードを入力します。
3. [New Password] (新しいパスワード) フィールドに新しいパスワードを入力します。[Confirm New Password] (新しいパスワードの確認) フィールドにパスワードを再入力します。パスワードには、最大 64 文字の英数字と特殊文字を使用できます。
4. [OK] をクリックします。
5. パスワードが正常に変更された旨のメッセージが表示されます。[OK] をクリックします。

注:強力なパスワードが使用されている場合は、パスワードに必要な形式に関する情報がこのページに表示されます。パスワードと強力なパスワードについての詳細は、オンライン ヘルプの 「Strong Passwords (強力なパスワード) 』171*p.* の『[Strong Passwords] (強力なパスワード) "参照 』」*を参照してください。*



デバイス管理

ネットワーク設定

[Network Settings] (ネットワーク設定) ページを使用して、KX III のネットワーク設定 (たとえば、IP アドレス、検出ポート、LAN インタフェース パラメータなど) をカスタマイズします。

IP 設定を行うには 2 つのオプションがあります。

- [None] (なし) (デフォルト) – 推奨されるオプションです (静的 IP)。KX III はネットワーク インフラストラクチャの一部であるため、IP アドレスを頻繁に変更されると手間がかかります。このオプションにより、ネットワーク パラメータを固定できます。
- [DHCP] (DHCP) – DHCP サーバによって IP アドレスが自動的に割り当てられます。

► **ネットワーク設定を変更するには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. ネットワーク基本設定を更新します。「*ネットワーク基本設定*『*84*p. 』」を参照してください。
3. LAN インタフェースの設定を更新します。「*LAN インタフェース設定* 『*88*p. 』」を参照してください。
4. [OK] (OK) をクリックして、これらの設定を保存します。変更を適用するために再起動が必要な場合は、再起動メッセージが表示されます。

► **工場出荷時のデフォルトに戻すには、以下の手順に従います。**

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

ネットワーク基本設定

ここでは、[Network Settings] (ネットワーク設定) ページで IP アドレスを割り当てる方法について説明します。このページのすべてのフィールドおよび操作についての詳細は、「*ネットワーク設定* 『*84*p. 』」を参照してください。

► **IP アドレスを割り当てるには、次の手順に従います。**

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. KX III デバイスにわかりやすいデバイス名を指定します。最大 32 文字の英数字と有効な特殊文字を組み合わせて使用できます。スペースは使用できません。
3. [IPv4] (IPv4) セクションで、IPv4 固有の適切なネットワーク設定を入力するか、選択します。

a. 必要に応じて IP アドレスを入力します。デフォルトの IP アドレスは「192.168.0.192」です。

b. サブネット マスクを入力します。デフォルトのサブネット マスクは「255.255.255.0」です。

c. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [None] (なし) を選択した場合は、デフォルトのゲートウェイを入力します。

d. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [DHCP] (DHCP) を選択した場合は、優先ホスト名を入力します。

e. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。

- [None] (なし) (静的 IP) - このオプションを選択した場合は、ネットワーク パラメータを手動で指定する必要があります。

  KX III はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、このオプションが推奨されます。

- [DHCP] (DHCP) - DHCP サーバから一意の IP アドレスとその他のパラメータを取得するために、ネットワークに接続しているコンピュータ (クライアント) によって Dynamic Host Configuration Protocol が使用されます。

  このオプションを選択した場合、ネットワーク パラメータは DHCP サーバによって割り当てられます。DHCP を使用する場合は、[Preferred host name] (優先ホスト名) を入力します (DHCP のみ)。最大 63 文字まで使用できます。

4. IPv6 を使用する場合は、[IPv6] セクションで、適切な IPv6 固有のネットワーク設定を入力するか、選択します。

a. セクション内のフィールドを有効にするには、[IPv6] チェックボックスをオンにします。

b. [Global/Unique IP Address] (グローバル/一意の IP アドレス) を入力します。これは、KX III に割り当てられる IP アドレスです。

c. [Prefix Length] (固定長) を入力します。これは、IPv6 アドレスで使用されるビット数です。

d. [Gateway IP Address] (ゲートウェイ IP アドレス) を入力します。

e. [Link-Local IP Address] (リンク - ローカル IP アドレス)。このアドレスは、自動的にデバイスに割り当てられます。これは、近隣探索、またはルータが存在しない場合に使用されます。**[Read-Only] (読み取り専用)**

f. [Zone ID]。これは、アドレスが関連付けられているデバイスを識別します。**[Read-Only] (読み取り専用)**

g. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。

- [None] (設定しない) – 自動 IP 設定を使用せず、IP アドレスを自分で設定する場合は、このオプションを選択します (静的 IP)。推奨されるデフォルトのオプションです。

  [IP auto configuration] (IP 自動設定) で [None] (設定しない) を選択すると、[Network Basic Settings] (ネットワーク基本設定) フィールド ([Global/Unique IP Address] (グローバル/一意の IP アドレス)、[Prefix Length] (固定長)、[Gateway IP Address] (ゲートウェイ IP アドレス)) が有効になり、IP アドレスを手動で設定できるようになります。
- [Router Discovery] (ルータ検出) – このオプションを使えば、グローバルな IPv6 アドレスまたは、ローカルにリンクしたアドレスを大きく超えるユニーク ローカルの IPv6 に自動的に割り当てられます。これはサブネットへの直接接続に限定して適用されます。

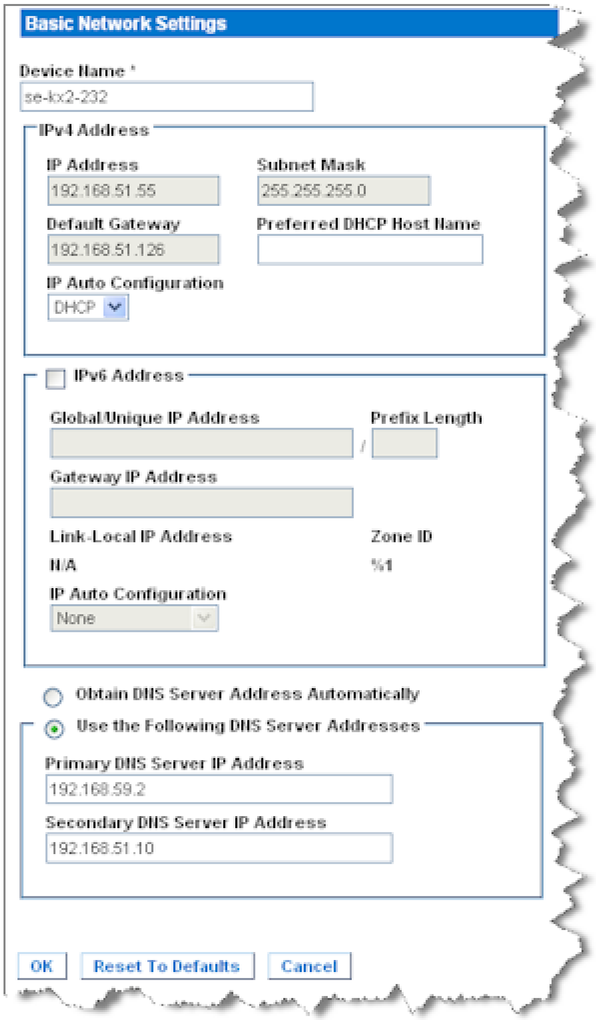
5. [DHCP] が選択され、[Obtain DNS Server Address] (DNS サーバ アドレスを取得) が有効になっている場合は、[Obtain DNS Server Address Automatically] (DNS サーバ アドレスを自動的に取得) を選択します。[Obtain DNS Server Address Automatically] (DNS サーバ アドレスを自動的に取得) が選択されると、DHCP サーバが提供する DNS 情報が使用されます。
6. [Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用) を選択する場合は、[DHCP] が選択されているかどうかにかかわらず、このセクションに入力されたアドレスが、DNS サーバの接続に使用されます。

   [Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用) オプションを選択する場合は、次の情報を入力します。これらのアドレスは、停電によりプライマリ DNS サーバ接続が切断された場合に使用されるプライマリおよびセカンダリ DNS アドレスです。

   a. [Primary DNS Server IP Address] (プライマリ DNS サーバ IP アドレス)
   b. [Secondary DNS Server IP Address] (セカンダリ DNS サーバ IP アドレス)
7. 完了したら [OK] をクリックします。

[Network Settings] (ネットワーク設定) ページのこのセクションの設定についての詳細は、「*LAN インタフェース設定* 『*88*p. 』」を参照してください。

注: 一部の環境では、[LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) のデフォルトである [Autodetect] (自動検出) (自動ネゴシエーション) が選択されている場合にネットワーク パラメータが適切に設定されず、ネットワーク上の問題が発生する場合があります。そのような場合は、KX III の [LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) フィールドを [100 Mbps/Full Duplex] (またはネットワークに合ったオプション) に設定することで問題を解決できます。詳細は、「ネットワーク設定 『84*p. 』」*を参照してください。*



LAN インタフェース設定

現在のパラメータ設定は、[Current LAN interface parameters] (現在の LAN インタフェース パラメータ) フィールドで確認します。

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. 以下の [LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) のオプションから適切なものを選択します。
   - [Autodetect] (自動検出) (デフォルト オプション)
   - [10 Mbps/Half] (10 Mbps/半二重) - 両方の LED が点滅
   - [10 Mbps/Full] (10 Mbps/全二重) - 両方の LED が点滅
   - [100 Mbps/Half] (100 Mbps/半二重) - 黄色の LED が点滅
   - [100 Mbps/Full] (100 Mbps/半二重) - 黄色の LED が点滅
   - [1000 Mbps/Full] (1000 Mbps/全二重) (ギガビット) - 緑色の LED が点滅
   - [Half-duplex] (半二重) の場合、双方向の通信は可能ですが、一度に通信できるのは一方向だけです (同時に通信できません)。
   - [Full-duplex] (全二重) の場合、同時に双方向の通信が可能です。

   注:半二重または全二重で 10 Mbps で実行しているときに、問題が発生する場合があります。問題が発生した場合は、別の速度と二重化の設定を選択してください。

   詳細は、「*Network Speed Settings* 『*342*p. の"***ネットワーク速度の設定***"参照 』」を参照してください。

3. この [Enable Automatic Failover] (自動フェイルオーバを有効にする) チェックボックスをオンにすると、アクティブなネットワーク ポートに障害が発生した場合、KX III では 2 番目のネットワーク ポートを使用して、自動的にネットワーク接続を回復します。

   注: フェイルオーバ ポートは実際にフェイルオーバが発生するまで有効にならないので、ポートを監視しないか、フェイルオーバが発生した後にのみ監視するようにすることをお勧めします。

   このオプションを有効にすると、次の 2 つのフィールドが使用されます。

   - [Ping Interval (seconds)] (Ping インターバル (秒)) - Ping インターバルの設定により、KX III が指定されたゲートウェイへのネットワーク パスの状態をチェックする頻度が決まります。デフォルトの Ping インターバルは 30 秒です。
   - [Timeout (seconds)] (タイムアウト (秒)) - タイムアウトの設定により、指定されたゲートウェイにネットワーク接続経由でアクセスできなくなってからフェイルオーバが発生するまでの時間が決まります。

注: Ping インターバルとタイムアウトは、ローカル ネットワーク状態に合わせて最適な値に設定できます。タイムアウトは、送信する 2 つ以上の Ping 要求と返される応答に対応できるように設定する必要があります。たとえば、ネットワークの利用率が高いためにフェイルオーバの発生する確率が高い場合は、タイムアウトを Ping インターバルの 3 ～ 4 倍に延ばす必要があります。

4. 帯域幅を選択します。
5. [OK] をクリックして LAN 設定を適用します。

ポートの設定

[Port Configuration] (ポート設定) ページへのアクセス

▶ ポート設定にアクセスするには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。

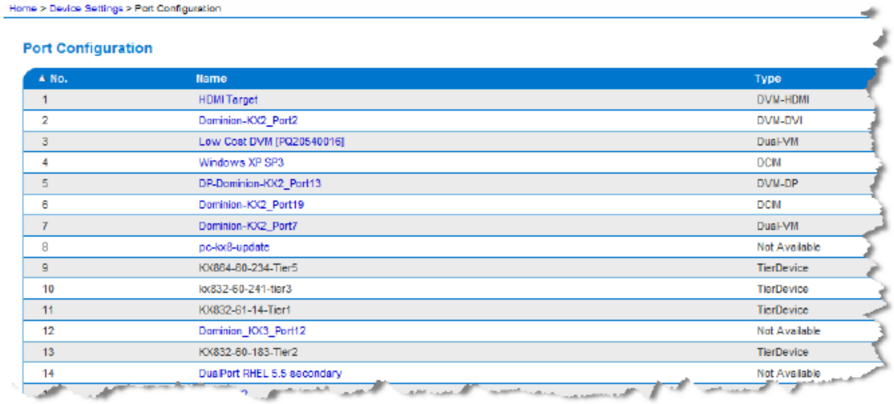
   最初このページはポートの番号順に表示されますが、列の見出しをクリックしてフィールドごとに並べ替えられます。
2. 編集するポートの [Port Name] (ポート名) をクリックします。
   - KVM ポートについては、KVM およびブレード シャーシ ポートの [Port] (ポート) ページが開きます。
   - ラック PDU については、ラック PDU (電源タップ) の [Port] (ポート) ページが開きます。このページで、ラック PDU とそれらのコンセントに名前を付けられます。

[Port Configuration] (ポート設定) ページ

[Port Configuration]（ポート設定）ページには、KX III のポートの一覧が表示されます。

ポートのステータスがダウンである場合、ステータスとして「Not Available」（使用不可）が表示されます。ポートの CIM が削除されているか電源が切られている場合、ポートがダウンになる可能性があります。

注:ブレード シャーシの場合、ブレード シャーシ名は変更できますが、そのブレード スロット名は変更できません。



Home > Device Settings > Port Configuration

Port Configuration

No.	Name	Type
1	HDMI Target	DVM-HDMI
2	Dominion-KX2_Port2	DVM-DVI
3	Low Cost DVM [PQ20540016]	Dual-VM
4	Windows XP SP3	DCIM
5	DP-Dominion-KX2_Port13	DVM-DP
6	Dominion-KX2_Port19	DCIM
7	Dominion-KX2_Port7	Dual-VM
8	pc-kx8-update	Not Available
9	KX864-60-234-Tier5	TierDevice
10	kx832-60-241-tier3	TierDevice
11	KX832-61-14-Tier1	TierDevice
12	Dominion_KX3_Port12	Not Available
13	KX832-60-183-Tier2	TierDevice
14	DualPort RHEL 5.5 secondary	Not Available

ポート番号

1 から、KX III デバイスで使用できるポートの合計数までの番号が振られています。

ポート名

CIM が接続されていないか、CIM 名が空白になっているポートには、デフォルト ポート名「」が割り当てられます。「Port#」は KX III の物理ポートの番号を表します。

現在 CIM を介して KX III に接続されていないポートのステータスは、[Not Available] (使用不可) になっています。

[Not Available] (使用不可) ステータスのポートの名前を変更するには、以下のいずれかの手順に従います。

- ポートの名前を変更します。CIM が接続されると、その CIM 名が使用されます。
- ポート名を変更し、[Persist name on Next CIM Insertion] (次回の CIM 挿入時に名前を維持) を選択します。CIM が接続されると、割り当てられている名前が CIM にコピーされます。
- [Reset to Defaults] (デフォルトに戻す) を選択して、ポート (名前を含む) を工場出荷時のデフォルトに戻します。CIM が接続されると、その CIM 名が使用されます。

注:ポート (CIM) 名にアポストロフィ (" ' ") を使用することはできません。

ポートの名前を変更した後でも、[Reset to Default] (デフォルトに戻す) 機能を使用すれば、いつでもデフォルトのポート名に戻ります。

ポート名をデフォルトにリセットすると、既存の電源の関連付けが削除され、さらにポートがポート グループに含まれている場合は、そのグループから削除されます。

[Port Type] (ポート タイプ)

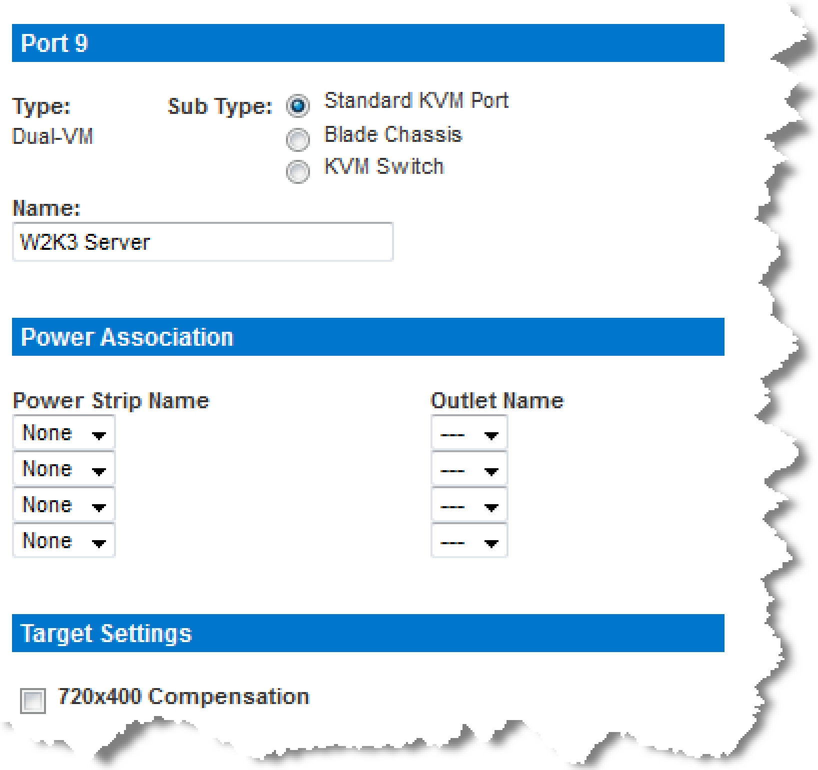
ポート タイプには、以下のものがあります。

- [DCIM] (DCIM) – Dominion CIM
- [TierDevice] (TierDevice) – カスケード接続デバイス
- [Not Available] (使用不可) – CIM の接続不可
- [DVM-DP] (DVM-DP) – 表示ポート CIM
- [DVM-HDMI] (DVM-HDMI) – HDMI CIMsw
- [DVM-DVI] (DVM-DVI) – DVI CIM
- [PowerStrip (rack PDU)] (電源タップ (ラック PDU)) – 電源タップを接続済み
- [VM] (VM) – D2CIM – VUSB CIM
- [Dual – VM] (デュアル – VM) – D2CIM – VUSB CIM
- [Blade Chassis] (ブレード シャーシ) – ブレード シャーシとそのシャーシに関連付けられているブレード (階層順に表示)
- [KVM Switch] (KVM スイッチ) – 汎用 KVM スイッチ接続
- [PCIM] (PCIM) – Paragon CIM

標準ターゲット サーバの設定

▶ ターゲット サーバに名前を付けるには、以下の手順に従います。

1. まだすべてのターゲット サーバを接続していない場合は、接続します。装置の接続方法の詳細は、「手順 3: 装置の接続」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。
3. 名前を変更するターゲット サーバのポート名をクリックします。[Port] (ポート) ページが開きます。
4. ポートのサブタイプとして [標準 KVM ポート] を選択します。
5. 当該ポートに接続されているサーバを識別するための名前を割り当てます。名前には最大 32 文字の英数字と特殊文字を使用できます。
6. [OK] をクリックします。



KVM スイッチを設定する

KX III では、ホット キー シーケンスを使用してターゲットを切り替えることもできます。ホット キー シーケンスを使用して標準サーバを切り替えることができるだけでなく、ブレード シャーシに対しても、また、カスケード接続構成でも KVM 切り替えが可能です。

重要: 作成する KVM スイッチがユーザ グループに表示されるようにするには、まずスイッチを作成してから、グループを作成する必要があります。作成中の KVM スイッチが既存のユーザ グループに表示されるようにする必要がある場合は、ユーザ グループを再作成する必要があります。

KVM スイッチを設定するには

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。
2. 名前を変更するターゲット サーバのポート名をクリックします。[Port] (ポート) ページが開きます。
3. [KVM Switch] (KVM スイッチ) を選択します。
4. KVM スイッチのモデルを選択します。

注: ドロップダウン リストにはスイッチが 1 つしか表示されません。

5. [KVM Switch Hot Key Sequence] (KVM 切り替えホット キー シーケンス) を選択します。
6. ターゲット ポートの最大数を 2 ～ 32 の範囲で入力します。
7. [KVM Switch Name] (KVM スイッチ名) フィールドに、このポート接続を参照する際に使用する名前を入力します。
8. KVM スイッチ ホット キー シーケンスを適用するターゲットをアクティブ化します。KVM スイッチ ポートにターゲットが接続されていることを示すため、各ポートに対して [Active] (アクティブ) を選択します。
9. このページの [KVM Managed Links] (KVM 管理下リンク) セクションで、Web ブラウザ インタフェースを使用できる場合にその Web ブラウザ インタフェースへの接続を設定できます。

a. [Active] (アクティブ) - 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。

b. [URL Name] (URL 名) - インタフェースの URL を入力します。

c. [Username] (ユーザ名) - インタフェースへのアクセスに使用されるユーザ名を入力します。

d. [Password] (パスワード) - インタフェースへのアクセスに使用されるパスワードを入力します。

e. [Username Field] (ユーザ名フィールド) - URL で使用されるユーザ名パラメータを入力します。たとえば、「*username*=admin」と入力します。*username* はユーザ名フィールドです。

f. [Password Field] (パスワード フィールド) - URL で使用されるパスワード パラメータを入力します。たとえば、「*passname*=raritan」と入力します。*passname* はパスワード フィールドです。

10. [OK] (OK) をクリックします。

▶ KVM スイッチ ポートまたは URL のアクティブ ステータスを変更するには

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。
2. 名前を変更するターゲット サーバのポート名をクリックします。[Port] (ポート) ページが開きます。
3. KVM スイッチ ターゲット ポートまたは URL の [Active] (アクティブ) チェック ボックスをオフにし、アクティブ ステータスを変更します。
4. [OK] (OK) をクリックします。

CIM ポートの設定

KX III では、標準の CIM および仮想メディア CIM を使用して、サーバを KX III に接続できます。

▶ CIM を設定するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。

2. 名前を変更するターゲット サーバのポートのポート名をクリックします。[Port] (ポート) ページが開きます。
3. ポートのサブタイプとして [標準 KVM ポート] を選択します。
4. 当該ポートに接続されているサーバを識別するための名前を割り当てます。名前には最大 32 文字の英数字と特殊文字を使用できます。
5. 必要な場合は、[Power Association] (電源の関連付け) セクションで、電源タップをポートに関連付けます。
6. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
7. デジタル CIM の場合、モニタ本来の表示解像度に合わせてターゲットの表示解像度を設定するには、[Display Native Resolution] (本来の表示解像度) ドロップダウンから解像度を選択します。

   HDMI CIM を使用している場合、オペレーティング システムとビデオ カードの組み合わせによっては、RGB 値の範囲が限られることがあります。[DVI Compatibility Mode] (DVI 互換モード) チェックボックスをオンにすると、色の範囲が拡大されます。
8. [OK] をクリックします。

ラック PDU (電源タップ) の接続先の設定

KX III では、ラック PDU (電源タップ) を KX III ポートに接続できます。

KX III のラック PDU の設定は、KX III の [Port Configuration] (ポート設定) ページから行います。

注:パフォーマンスが低下するおそれがあるので、KX III に接続するラック PDU (電源タップ) は 8 つ以下にすることをお勧めします。

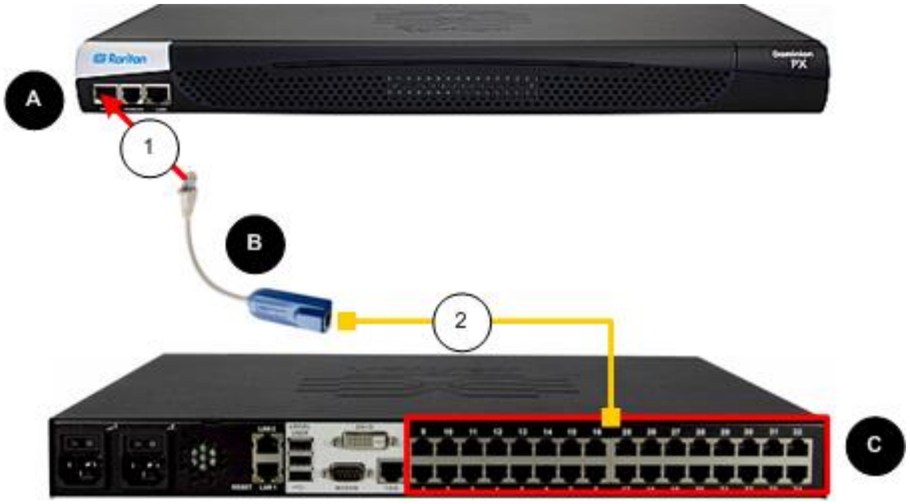
ラック PDU の接続

Raritan PX シリーズのラック PDU (電源タップ) は、D2CIM-PWR CIM を使用して Dominion デバイスに接続されます。

▶ ラック PDU に接続するには、以下の手順に従います。

1. D2CIM-PWR のオス RJ-45 を、ラック PDU のシリアル ポートのメス RJ-45 コネクタに接続します。
2. Cat5 ストレート ケーブルを使用して、D2CIM-PWR のメス RJ-45 コネクタを KX III で空いているメスのシステム ポート コネクタのいずれかに接続します。
3. AC 電源コードをターゲット サーバと空いているラック PDU コンセントに接続します。
4. ラック PDU を AC 電源に接続します。

5. デバイスの電源をオンにします。



図の説明	
A	シリアル ポートを搭載した PX ラック PDU
B	D2CIM-PWR
C	KX III
1	D2CIM-PWR とラック PDU シリアル ポートの接続
2	Cat5 ケーブルによる D2CIM-PWR と KX III ターゲット サーバ ポートの接続

ラック PDU の名前の指定 (電源タップの [Port] (ポート) ページ)

注:PX ラック PDU (電源タップ) の名前は、PX および KX III で指定できます。

Raritan リモート ラック PDU が KX III に接続されると、[Port Configuration] (ポート設定) ページに表示されます。そのページにある電源ポート名をクリックしてアクセスします。[Type] (タイプ) フィールドと [Name] (名前) フィールドには、あらかじめ入力されています。

注:(CIM) [Type] (タイプ) は変更できません。

ラック PDU の各コンセントに関する次の情報が表示されます。コンセントの [Number] (番号)、[Name] (名前)、[Port Association] (ポートの関連付け)。

このページを使用して、ラック PDU とそのコンセントに名前を付けます。名前には最大 32 文字の英数字が使用でき、特殊文字を含めることができます。

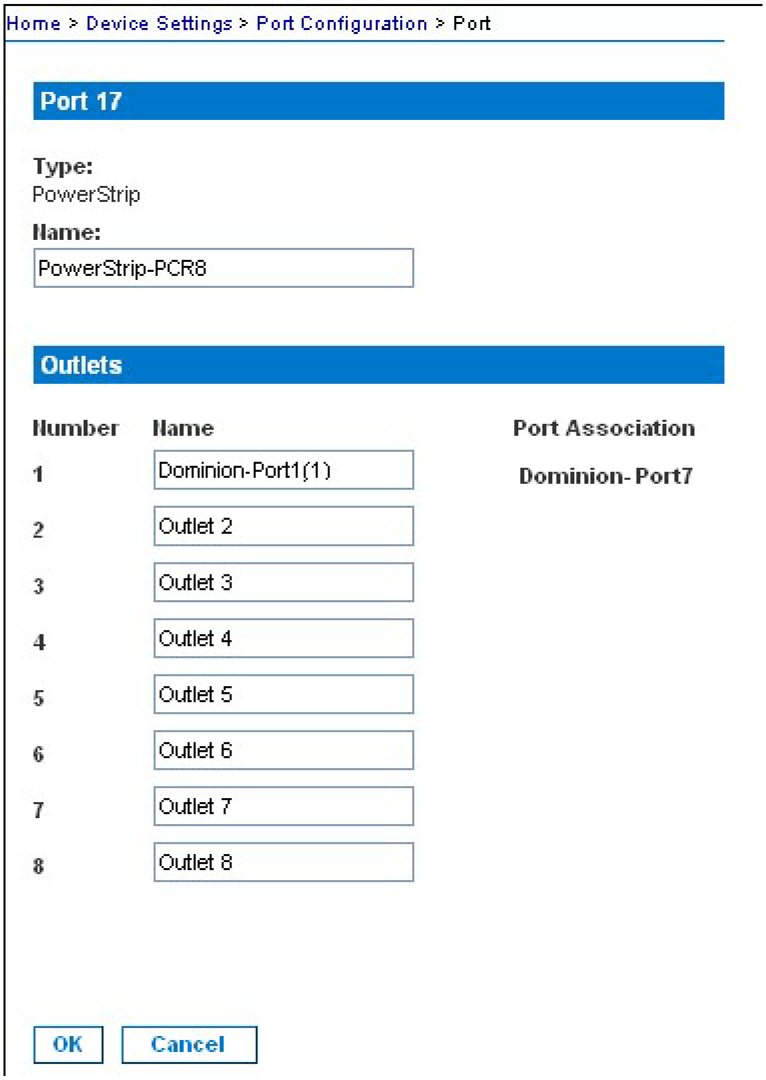
注:ラック PDU がターゲット サーバ (ポート) と関連付けられると、コンセント名はターゲット サーバ名に置き換えられます。コンセントに別の名前を割り当てている場合も同様です。

▶ ラック PDU およびコンセントに名前を付けるには、以下の手順に従います。

注:CommandCenter Secure Gateway では、スペースを含むラック PDU 名を認識できません。

1. ラック PDU の名前を入力します (必要な場合)。
2. 必要に応じて、([コンセント]) [Name] (名前) を変更します (デフォルトのコンセント名は、「outlet #」です)。

3. ［OK］をクリックします。



コンセントとターゲット サーバとの関連付け

[Port Configuration] (ポート設定) ページでポートをクリックすると、[Port] (ポート) ページが開きます。

ポートが接続されているサーバにコンセントを接続すると、電源をターゲット サーバに関連付けることができます。

サーバには最大で 4 つの電源プラグを接続でき、それぞれに別のラック PDU (電源タップ) を関連付けられます。このページでそれらの関連付けを定義して、[Port Access] (ポート アクセス) ページからサーバの電源オン、電源オフ、電源オン・オフを行えます。

この機能を使用するには、次のアイテムが必要です。

- Raritan リモート ラック PDU
- Power CIM (D2CIM-PWR)

電源の関連付け

▶ **電源の関連付けを行う (ラック PDU コンセントを KVM ターゲット サーバに関連付ける) には、以下の手順に従います。**

注:ラック PDU がターゲット サーバ (ポート) に関連付けられると、コンセント名はターゲット サーバ名に置き換えられます (コンセントに別の名前を割り当てている場合も同様です)。

---

1. [Port Configuration] (ポート設定) ページで、PDU に関連付けるターゲット サーバを選択します。
2. [Power Strip Name] (電源タップ名) ドロップダウン リストからラック PDU を選択します。
3. そのラック PDU に対して、[Outlet Name] (コンセント名) ドロップダウン リストからコンセントを選択します。
4. 該当するすべての電源の関連付けで、手順 1 および 2 を繰り返します。
5. [OK] をクリックします。確認メッセージが表示されます。

電源の関連付けの削除

ターゲット サーバやラック PDU をデバイスから取り外す場合は、まずすべての電源の関連付けを削除する必要があります。ターゲットがラック PDU に関連付けられたままでターゲットをデバイスから取り外した場合、電源の関連付けは残ります。この場合、電源の関連付けを適切に削除するために [Device Settings] (デバイス設定) で切断されたターゲット サーバの [Port Configuration] (ポート設定) にアクセスすることはできません。

▶ **ラック PDU の関連付けを削除するには、次の手順に従います。**

1. [Power Strip Name] (電源タップ名) ドロップダウン リストから適切なラック PDU を選択します。

2. そのラック PDU に対して、[Outlet Name] (コンセント名) ドロップダウン リストから適切なコンセントを選択します。
3. [Outlet Name] (コンセント名) ドロップダウン リストから、[None] (設定なし) を選択します。
4. [OK] をクリックします。そのラック PDU/コンセントの関連付けが削除され、確認メッセージが表示されます。

▶ **ラック PDU がターゲットから削除されている場合にラック PDU の関連付けを削除するには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) をクリックし、アクティブなターゲットをクリックします。
2. アクティブなターゲットを、切断された電源ポートに関連付けます。これで、切断されたターゲットの電源の関連付けが破棄されます。
3. 最後に、アクティブなターゲットを、正しい電源ポートに関連付けます。

ブレード シャーシの設定

標準型サーバとラック PDU (電源タップ) に加えて、KX III のポートに接続されているブレード シャーシを制御することができます。一定時間に最大 8 台のブレード シャーシを管理できます。

ブレード シャーシ タイプがサポートされている場合、ブレード シャーシは、接続されると自動的に検出されます。

ブレード シャーシが検出された場合は、デフォルト名が関連付けられ、それが [Port Access] (ポート アクセス) ページに、標準ターゲット サーバおよびラック PDU と共に表示されます。

シャーシ タイプがサポートされていない場合は、そのブレードを手動で設定する必要があります。ブレード シャーシは、ブレード シャーシ サブタイプとして設定する必要があります。

ブレードの表示方法の詳細については、「*[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)*『*17*p. 』」を参照してください。

ブレード シャーシ設定オプション

HP ブレード シャーシおよび Cisco® UCS ブレード シャーシを除く、汎用、IBM®、Dell® の各ブレード シャーシは、[Port Access] (ポート アクセス) ページで設定されます。

ブレード シャーシに接続されるポートは、ブレード シャーシ モデルで設定されている必要があります。

ブレード サーバに設定できる特定の情報は、使用しているブレード サーバのブランドによって異なります。サポートされているこれらの各ブレード シャーシ固有の情報は、このセクションのヘルプにある対応するトピックを参照してください。

Dell

- Dell PowerEdge® 1855、1955、および M1000e

  Dell PowerEdge 1855/1955 ブレードも、各個別ブレードから Dominion デバイス上のポートに接続できます。この方法で接続した場合、それらをグループ化してブレード サーバ グループを作成できます。

IBM

- IBM BladeCenter® モデル E および H

Generic (汎用)

- [Generic] (汎用) オプションでは、Dell PowerEdge® 1855、1955、および M1000e、IBM BladeCenter® モデル E および H、HP BladeSystem c3000 および c7000、Cisco UCS ブレード サーバ以外のブレード シャーシを設定できます。

HP

- HP BladeSystem c3000 と c7000 のブレード サーバ、および Cisco UCS ブレード サーバは、Dominion デバイスから各ブレードへの個別の接続を介してサポートされます。

  ポートは、ポート グループ管理機能を使用して、シャーシにまとめてグループ化されます。

ブレード シャーシの手動検出および自動検出の設定

ブレード シャーシでは、手動設定と自動検出の 2 つの操作モードがあり、ブレード シャーシの機能によって決まります。

ブレード シャーシが自動検出で設定される場合、Dominion デバイスは、以下を追跡および更新します。

- 新しいブレード サーバがいつシャーシに追加されるか。
- 既存のブレード サーバがいつシャーシから削除されるか。

注: IBM Blade Center モデル E および H を使用する場合、KX III では、プライマリ管理モジュールとして AMM[1] の自動検出のみサポートされます。

ブレード シャーシにアクセスするためのホットキー シーケンス

ホット キー シーケンスを使用してブレード シャーシへの KVM アクセスを切り替えることもできます。

ユーザがホットキー シーケンスを選択できるブレード シャーシの場合、これらのオプションは、[Port Configuration]（ポート設定）ページにあります。

ホットキー シーケンスがあらかじめ定義されているブレード シャーシの場合、これらのシーケンスは、ブレード シャーシが選択されると [Port Configuration]（ポート設定）ページに自動的に入力されます。

たとえば、IBM BladeCenter H に対する KVM を切り替えるためのデフォルト ホットキー シーケンスは、NumLock+NumLock+SlotNumber なので、設定中に IBM BladeCenter H が選択されたときに、このホットキー シーケンスがデフォルトで適用されます。ホットキー シーケンスについての詳細は、ブレード シャーシのマニュアルを参照してください。

ブレード シャーシ インタフェースへのリンク

ブレード シャーシ Web ブラウザ インタフェースがある場合は、それに対する接続を設定できます。シャーシ レベルでは、最大 4 つのリンクを定義できます。

1 つ目のリンクは、ブレード シャーシ管理モジュール GUI への接続用に予約されています。

たとえば、このリンクは、テクニカル サポートがシャーシ設定をすばやく検証する場合に使用されることがあります。

ブレード シャーシの管理

ブレード シャーシは、Virtual KVM Client (VKC)、Active KVM Client (AKC)、および CC-SG から管理できます。

VKC および AKC を介したブレード サーバの管理は、標準ターゲット サーバの管理と同じです。

詳細については、ユーザ ヘルプおよび『**CC-SG 管理者ガイド**』を参照してください。

注:ブレード シャーシ設定に対する変更は、これらのクライアント アプリケーションに反映されます。

重要: ブレード シャーシを Dominion デバイスに CIM 接続することによって、電源がオフになったり Dominion デバイスから切断されたりした場合、ブレード シャーシに対して確立されているすべての接続が切断されます。CIM が再接続されるか電源オンにした場合は、接続を再確立する必要があります。

汎用ブレード シャーシの設定

[Generic] (汎用) ブレード シャーシを選択した場合の操作モードは、手動設定モードだけです。 ブレード シャーシを設定する際の重要な情報および追加情報については、「***サポートされているブレード シャーシ モデル***『***119***p. 』」、「***ブレード シャーシでサポートされている CIM***『***120***p. 』」、および「***ブレード シャーシの必須および推奨設定***『***123***p. 』」を参照してください。Dell® のシャーシで KX III を使用する場合のケーブルの長さとビデオ解像度の詳細については、「***Dell シャーシを接続する場合のケーブル長と画面解像度***『***344***p. の"***Dell 筐体を接続する場合のケーブル長と画面解像度***"参照 』」を参照してください。

▶ シャーシを設定するには、以下の手順に従います。

1. ブレード シャーシを KX III に接続します。装置の接続方法の詳細は、「手順 3: 装置の接続」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Settings] (ポート設定) をクリックし、[Port Settings] (ポート設定) ページを開きます。
3. [Port Settings] (ポート設定) ページで、設定するブレード シャーシの名前をクリックします。[Port] (ポート) ページが開きます。
4. [Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択します。ページに、ブレード シャーシの設定に必要なフィールドが表示されます。
5. [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストから [Generic] (汎用) を選択します。
6. ブレード シャーシを適切に設定します。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード シャーシへの切り替えに使用されるホットキー シーケンスを定義します。[Switch Hot Key Sequence] (切り替えホットキー シーケンス) は、ブレード シャーシの KVM モジュールで使用されるシーケンスと同じにする必要があります。
   b. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - 適用されません。
   c. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数を入力します。
   d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。 適用されません。
   e. [User Name] (ユーザ名) - 適用されません。
   f. [Password] (パスワード) - 適用されません。
7. 必要に応じてブレード シャーシ名を変更します。

8. ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。
9. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン

をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

---

   a. [Active] (アクティブ) - 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。
   b. [URL] (URL) - インタフェースへの URL を入力します。 **必ず入力してください。**
   c. [Username] (ユーザ名) - インタフェースへのアクセスに使用されるユーザ名を入力します。 **(オプション)**
   d. [Password] (パスワード) - インタフェースへのアクセスに使用されるパスワードを入力します。 **(オプション)**

注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のまましないと、接続が失敗します。

---

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「***Web ブラウザ インタフェースの追加に関するヒント*** 『*115*p. 』」を参照してください。**(オプション)**

10. USB プロファイル情報は汎用設定には適用されません。
11. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
12. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。

CIM の本来の表示解像度を [Display Native Resolution] (本来の表示解像度) ドロップダウンから選択します。これは、デジタル CIM の優先の解像度およびタイミング モードです。解像度は、選択されたら、CIM に適用されます。

1. 選択されない場合は、デフォルトの解像度 1280 x 1024、60 Hz が使用されます。
2. [OK] をクリックして設定を保存します。

Dell ブレード シャーシの設定

ブレード シャーシを設定する際の重要な情報および追加情報については、「***サポートされているブレード シャーシ モデル*** 『*119*p. 』」、「***ブレード シャーシでサポートされている CIM*** 『*120*p. 』」、および「***ブレード シャーシの必須および推奨設定*** 『*123*p. 』」を参照してください。Dell® のシャーシで KX III を使用する場合のケーブルの長さとビデオ解像度の詳細については、「***Dell シャーシを接続する場合のケーブル長と画面解像度*** 『*344*p. の"***Dell 筐体を接続する場合のケーブル長と画面解像度***"参照 』」を参照してください。

▶ ブレード シャーシを追加するには、以下の手順に従います。

1. ブレード シャーシを KX III に接続します。装置の接続方法の詳細は、「手順 3: 装置の接続」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Settings] (ポート設定) をクリックし、[Port Settings] (ポート設定) ページを開きます。
3. [Port Settings] (ポート設定) ページで、設定するブレード シャーシの名前をクリックします。[Port] (ポート) ページが開きます。

4. [Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択します。ページに、ブレード シャーシの設定に必要なフィールドが表示されます。
5. [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストから Dell ブレード シャーシ モデルを選択します。

Dell PowerEdge M1000e を設定するには、以下の手順に従います。

1. [Dell PowerEdge™ M1000e] (Dell PowerEdge M1000e) を選択した場合は、自動検出を使用できます。ブレード シャーシを適切に設定します。自動検出できるブレード シャーシを設定する前に、指定されたポート番号で SSH 接続を有効に設定する必要があります (「[Device Services] (デバイス サービス)」を参照してください)。また、対応する認証証明書を持つユーザ アカウントを、ブレード シャーシであらかじめ作成しておく必要があります。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) – KVM からブレード サーバへの切り替えに使用されるホットキー シーケンスを選択します。 [Switch Hot Key Sequence] (切り替えホットキー シーケンス) は、ブレード シャーシの KVM モジュールで使用されるシーケンスと同じにする必要があります。
   b. [Maximum Number of Slots] (最大スロット数) – ブレード シャーシで使用できるデフォルトの最大スロット数は、自動的に入力されます。
   c. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) – ブレード シャーシのプライマリ IP アドレスを入力します。 **自動検出モードでは必須です。**
   d. [Port Number] (ポート番号) – ブレード シャーシのデフォルトのポート番号は 22 です。必要に応じて、ポート番号を変更します。**自動検出モードでは必須です。**
   e. [Username] (ユーザ名) – ブレード シャーシへのアクセスに使用されるユーザ名を入力します。 **自動検出モードでは必須です。**
   f. [Password] (パスワード) – ブレード シャーシへのアクセスに使用されるパスワードを入力します。 **自動検出モードでは必須です。**
2. KX III でシャーシ ブレードを自動検出する場合は、[Blade Auto-Discovery] (ブレードの自動検出) チェックボックスをオンにし、[Discover Blades on Chassis Now] (ブレード シャーシを今すぐ検出) をクリックします。ブレードが検出されると、それがページに表示されます。

3. 必要に応じてブレード シャーシ名を変更します。シャーシに既に名前が付けられている場合は、その情報がこのフィールドに自動的に表示されます。まだ名前が付いていない場合は、KX III によってシャーシに名前が割り当てられます。KX III では、ブレード シャーシにデフォルトで「Blade_Chassis_Port#」という名前が付けられます。
4. 手動モードで操作する場合は、ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。

   自動検出モードで操作する場合は、[Installed] (インストール済み) チェックボックスに、検出中にブレードを含んでいたスロットが表示されます。
5. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ► Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

   注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

   ---

   a. [Active] (アクティブ) - 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。
   b. [URL] (URL) - インタフェースへの URL を入力します。 Dell M1000e のサンプル設定の詳細は、「***ブレード シャーシのサンプル URL フォーマット*** 『*125*p. 』」を参照してください。
   c. [Username] (ユーザ名) - インタフェースへのアクセスに使用されるユーザ名を入力します。
   d. [Password] (パスワード) - インタフェースへのアクセスに使用されるパスワードを入力します。

注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のまましないと、接続が失敗します。

---

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「***Web ブラウザ インタフェースの追加に関するヒント*** 『*115*p. 』」を参照してください。

6. USB プロファイルは Dell シャーシには適用されません。
7. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
8. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。

CIM の本来の表示解像度を [Display Native Resolution] (本来の表示解像度) ドロップダウンから選択します。これは、デジタル CIM の優先の解像度およびタイミング モードです。解像度は、選択されたら、CIM に適用されます。

1. 選択されない場合は、デフォルトの解像度 1280 x 1024、60 Hz が使用されます。
2. [OK] をクリックして設定を保存します。

▶ Dell PowerEdge 1855/1955 を設定するには、以下の手順に従います。

1. [Dell 1855/1955] (Dell 1855/1955) を選択した場合は、自動検出は*使用できません*。ブレード シャーシを適切に設定します。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード サーバへの切り替えに使用されるホットキー シーケンスを選択します。 Dell 1855/1955 モデルの場合は、KX III によって既存のすべてのホットキー シーケンスをブロックします。汎用設定を Dell 1855 に適用する場合は、既存のホットキー 1 つだけがブロックされます。

b. [Maximum Number of Slots] (最大スロット数) – ブレード シャーシで使用できるデフォルトの最大スロット数は、自動的に入力されます。

c. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) – 適用されません。

d. [Port Number] (ポート番号) – ブレード シャーシのデフォルトのポート番号は 22 です。 適用されません。

e. [User Name] (ユーザ名) – 適用されません。

f. [Password] (パスワード) – 適用されません。

2. 必要に応じてブレード シャーシ名を変更します。
3. ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。
4. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン

をクリックして、ページのセクションを展開します。

最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

---

a. [Active] (アクティブ) – 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。

b. [URL] (URL) – インタフェースへの URL を入力します。 Dell PowerEdge 1855/1955 のサンプル設定の詳細は、「ブレード シャーシのサンプル URL フォーマット」を参照してください。

c. [Username] (ユーザ名) – インタフェースへのアクセスに使用されるユーザ名を入力します。

d. [Password] (パスワード) – インタフェースへのアクセスに使用されるパスワードを入力します。

注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のまましないと、接続が失敗します。

---

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「***Web ブラウザ インタフェースの追加に関するヒント*** 『*115*p. 』」を参照してください。

5. USB プロファイルは Dell シャーシには適用されません。
6. [OK] をクリックして設定を保存します。

IBM ブレード シャーシの設定

ブレード シャーシを設定する際の重要な情報および追加情報については、「***サポートされているブレード シャーシ モデル*** 『*119*p. 』」、「***ブレード シャーシでサポートされている CIM*** 『*120*p. 』」、および「***ブレード シャーシの必須および推奨設定*** 『*123*p. 』」を参照してください。

Dell® のシャーシで KX III を使用する場合のケーブルの長さとビデオ解像度の詳細については、「***Dell シャーシを接続する場合のケーブル長と画面解像度*** 『*344*p. の"***Dell 筐体を接続する場合のケーブル長と画面解像度***"参照 』」を参照してください。

▶ **ブレード シャーシを追加するには、以下の手順に従います。**

1. ブレード シャーシを KX III に接続します。装置の接続方法の詳細は、「手順 3: 装置の接続」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Settings] (ポート設定) をクリックし、[Port Settings] (ポート設定) ページを開きます。
3. [Port Settings] (ポート設定) ページで、設定するブレード シャーシの名前をクリックします。[Port] (ポート) ページが開きます。
4. [Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択します。ページに、ブレード シャーシの設定に必要なフィールドが表示されます。
5. [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストから IBM® ブレード シャーシ モデルを選択します。

▶ IBM BladeCenter H および E を設定するには、以下の手順に従います。

1. IBM BladeCenter® H または E を選択した場合は、自動検出を使用できます。ブレード シャーシを適切に設定します。自動検出できるブレード シャーシを設定する前に、指定されたポート番号で SSH 接続を有効に設定する必要があります (「[Device Services] (デバイス サービス)」を参照してください)。また、対応する認証証明書を持つユーザ アカウントを、ブレード シャーシであらかじめ作成しておく必要があります。 KX III では、AMM[1] の自動検出のみサポートされます。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - 定義済みです。
   b. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数は、自動的に入力されます。
   c. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - ブレード シャーシのプライマリ IP アドレスを入力します。 **自動検出モードでは必須です。**
   d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。必要に応じて、ポート番号を変更します。**自動検出モードでは必須です。**
   e. [Username] (ユーザ名) - ブレード シャーシへのアクセスに使用されるユーザ名を入力します。 **自動検出モードでは必須です。**
   f. [Password] (パスワード) - ブレード シャーシへのアクセスに使用されるパスワードを入力します。 **自動検出モードでは必須です。**
2. KX III でシャーシ ブレードを自動検出する場合は、[Blade Auto-Discovery] (ブレードの自動検出) チェックボックスをオンにし、[Discover Blades on Chassis Now] (ブレード シャーシを今すぐ検出) をクリックします。ブレードが検出されると、それがページに表示されます。
3. 必要に応じてブレード シャーシ名を変更します。シャーシに既に名前が付けられている場合は、その情報がこのフィールドに自動的に表示されます。まだ名前が付いていない場合は、KX III によってシャーシに名前が割り当てられます。KX III では、ブレード シャーシにデフォルトで「Blade_Chassis_Port#」という名前が付けられます。
4. 手動モードで操作する場合は、ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。

自動検出モードで操作する場合は、[Installed] (インストール済み) チェックボックスに、検出中にブレードを含んでいたスロットが表示されます。

5. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン

をクリックして、ページのセクションを展開します。

最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

---

a. [Active] (アクティブ) - 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。

b. [URL] (URL) - インタフェースへの URL を入力します。 IBM BladeCenter のサンプル設定の詳細は、「***ブレード シャーシのサンプル URL フォーマット*** 『*125*p. 』」を参照してください。

c. [Username] (ユーザ名) - インタフェースへのアクセスに使用されるユーザ名を入力します。

d. [Password] (パスワード) - インタフェースへのアクセスに使用されるパスワードを入力します。

注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のまましないと、接続が失敗します。

---

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「*Web ブラウザ インタフェースの追加に関するヒント* 『*115*p. 』」を参照してください。

6. 適用できる場合は、ブレード シャーシの USB プロファイルを定義するか、既存の USB プロファイルを選択します。[Select USB Profiles for Port] (ポートの USB プロファイルを選択) アイコン

または [Apply Select Profiles to Other Ports] (選択したプロファイルを他のポートに適用) アイコン

をクリックして、ページ内のこのセクションを展開します。「*USB プロファイルの設定 ([Port] (ポート) ページ)* 『*127*p. 』」を参照してください。

7. [OK] をクリックして設定を保存します。

▶ IBM BladeCenter (その他) を設定するには、以下の手順に従います。

1. [IBM BladeCenter (Other)] (IBM BladeCenter (Other) を選択した場合は、自動検出は*使用できません*。ブレード シャーシを適切に設定します。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード サーバへの切り替えに使用されるホットキー シーケンスを選択します。
   b. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - ブレード シャーシのプライマリ IP アドレスを入力します。適用されません。
   c. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数を入力します。
   d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。 適用されません。
   e. [User Name] (ユーザ名) - 適用されません。
   f. [Password] (パスワード) - 適用されません。
2. 必要に応じてブレード シャーシ名を変更します。

3. ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。まだ名前が付いていない場合は、KX III によってブレード サーバに名前が割り当てられます。ブレード サーバにはデフォルトで「Blade_Chassis_Port#_Slot#」という名前が付けられます。
4. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン

をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

   注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

   ---

   a. [Active] (アクティブ) – 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。
   b. [URL] (URL) – インタフェースへの URL を入力します。 IBM BladeCenter のサンプル設定の詳細は、「***ブレード シャーシのサンプル URL フォーマット*** 『*125*p. 』」を参照してください。
   c. [Username] (ユーザ名) – インタフェースへのアクセスに使用されるユーザ名を入力します。
   d. [Password] (パスワード) – インタフェースへのアクセスに使用されるパスワードを入力します。

   注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のまましないと、接続が失敗します。

   ---

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「***Web ブラウザ インタフェースの追加に関するヒント*** 『*115*p. 』」を参照してください。

5. USB プロファイルは [IBM (Other)] (IBM (その他)) 設定では使用されません。
6. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
7. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。

CIM の本来の表示解像度を [Display Native Resolution] (本来の表示解像度) ドロップダウンから選択します。これは、デジタル CIM の優先の解像度およびタイミング モードです。解像度は、選択されたら、CIM に適用されます。

1. 選択されない場合は、デフォルトの解像度 1280 x 1024、60 Hz が使用されます。
2. [OK] をクリックして設定を保存します。

Web ブラウザ インタフェースの追加に関するヒント

Web ブラウザ インタフェースを追加して、埋め込み Web サーバを持つデバイスとの接続を作成できます。Web ブラウザ インタフェースは、RSA、DRAC、または ILO Processor カードに関連付けられている Web アプリケーションなどの任意の Web アプリケーションへの接続にも使用できます。

DNS を設定しておく必要があります。そうしないと、URL が解決されません。IP アドレスの場合は DNS を設定する必要はありません。

▶ Web ブラウザ インタフェースを追加するには、以下の手順に従います。

1. Web ブラウザ インタフェースのデフォルト名が提供されます。必要な場合は、[Name] (名前) フィールドで名前を変更します。
2. [URL] (URL) フィールドに Web アプリケーションの URL またはドメイン名を入力します。Web アプリケーションでユーザ名とパスワードの読み取りが行われる URL を入力する必要があります。

正しいフォーマットについては、以下の例を参照してください。

- http(s)://192.168.1.1/login.asp
- http(s)://www.example.com/cgi/login
- http(s)://example.com/home.html

3. このインタフェースへのアクセスが許可されるユーザ名とパスワードを入力します。**(オプション)**
4. ユーザ名とパスワードが入力された場合、[Username Field] (ユーザ名 フィールド) と [Password Field] (パスワード フィールド) に、Web アプリケーションのログイン画面で使用されるユーザ名フィールドとパスワード フィールドのフィールド名を入力します。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの名前を探す必要があります。

フィールド名検索に関するヒント:

- Web アプリケーションのログイン ページの HTML ソース コードで、Username や Password などのフィールドのラベルを検索します。
- フィールド ラベルが見つかったら、隣接するコードで "name="user"" のようなタグを探します。引用符内の語がフィールド名です。

HP および Cisco UCS のブレード シャーシ設定 (ポート グループ管理)

KX III は、特定のタイプのブレードに接続されるポートをまとめてブレード シャーシを示すグループとしてサポートします。特に、Cisco® UCS ブレード、HP® BladeServer ブレード、および Dell® PowerEdge™ 1855/1955 ブレード（Dell PowerEdge 1855/1955 ブレードが個別の各ブレードから KX III 上のポートに接続されている場合）がこれにあたります。

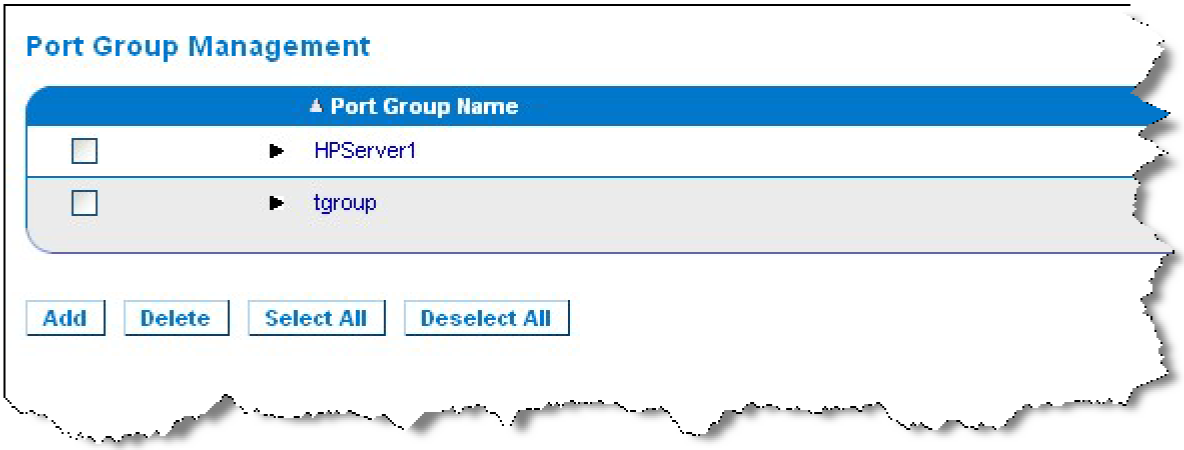
シャーシは、[Port Group Name]（ポート グループ名）によって特定され、グループは、[Port Group Management]（ポート グループ管理）ページの [Blade Server Group]（ブレード サーバ グループ）として指定されます。ポート グループには、標準 KVM ポートとして設定されたポートのみで構成され、ブレード シャーシとして設定されたポートは含まれません。ポートは、1 つのグループだけに属することができます。

ブレード シャーシで組み付けの KVM モジュールに接続されているポートは、ブレード シャーシ サブタイプとして設定されます。これらのポートは、ポート グループに含めることができます。

KX III ポートがブレード シャーシ内で組み付けの KVM モジュールに接続され、個別のブレードに接続されていない場合、ポートはブレード シャーシ サブタイプとして設定されます。これらのポートはポート グループに含めることはできないので、[Select Port for Group]（グループ化するポートの選択）の [Available]（利用可能）リストには表示されません。

ポート グループに含まれている標準 KVM ポートを、後でブレード シャーシ サブタイプとして用途変更する場合は、まず、ポート グループからそれを削除する必要があります。

ポート グループは、[Backup and Restore]（バックアップとリストア）オプションを使用してリストアされます（「*バックアップと復元*『*192*p. 』」を参照してください）。



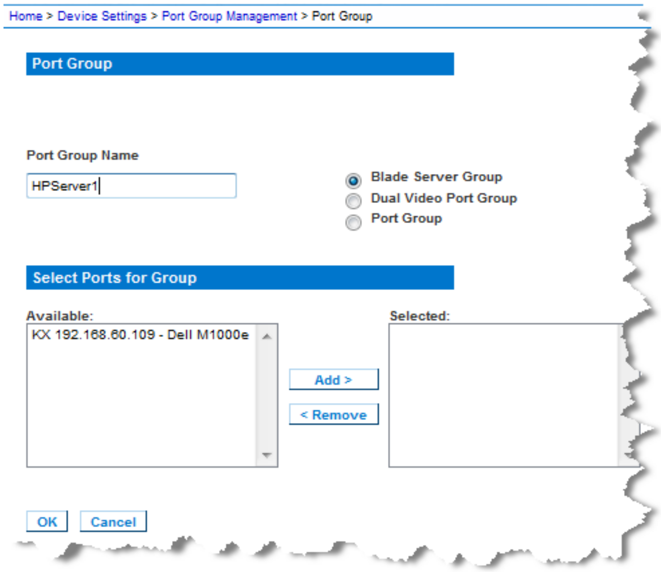
▶ ポート グループを追加するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Group Management] (ポート グループ管理) をクリックし、[Port Group Management] (ポート グループ管理) ページを開きます。
2. [Add] (追加) をクリックすると、[Port Group] (ポート グループ) ページが開きます。
3. ポート グループ名を入力します。ポート グループでは、最大 32 文字で、大文字と小文字は区別されません。
4. [Blade Server Group] (ブレード サーバ グループ) チェックボックスをオンにします。

   これらのポートをブレード シャーシ (たとえば、HP c3000 または Dell PowerEdge 1855) 内のブレードに接続するように指定する場合は、[Blade Server Group] (ブレード サーバ グループ) チェックボックスをオンにします。

   注:各ブレードは KX III のポートに独自に接続されていますが、これは、HP ブレードをシャーシ ベースで整理する CC-SG ユーザにとっては特に重要です。

   ---
5. [Select Ports for Group] (グループ化するポートの選択) セクションの [Available] (利用可能) ボックスで、ポートをクリックします。[Add] (追加) をクリックして、ポートをグループに追加します。ポートは [Selected] (選択) ボックスに移動されます。
6. [OK] をクリックして、ポート グループを追加します。



ポート グループ情報を編集するには、以下の手順に従います。

1. [Port Group Management] (ポート グループ管理) ページで、編集するポート グループのリンクをクリックします。[Port Group] (ポート グループ) ページが開きます。
2. 必要に応じて情報を編集します。
3. [OK] をクリックして変更を保存します。

ポート グループを削除するには、以下の手順に従います。

1. [Port Group Management] (ポート グループ管理) ページをクリックし、削除するポート グループのチェックボックスをオンにします。
2. [Delete] (削除) をクリックします。
3. 警告メッセージで [OK] をクリックします。

サポートされているブレード シャーシ モデル

この表には、KX III でサポートされているブレード シャーシ モデルと、それらを KX III アプリケーションで設定する際にシャーシごとに選択する必要がある対応プロファイルが含まれています。これらのモデルのリストは、[Port Configuration] (ポート設定) ページの [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストで選択できます。これは、[Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択している場合に表示されます。各ブレード シャーシ モデルの設定方法についての詳細は、このセクションのヘルプ内の対応するトピックを参照してください。

ブレード シャーシ モデル	KX III プロファイル
Cisco® UCS	ポート グループ管理機能を使用して設定します。「*HP および Cisco UCS のブレード シャーシ設定 (ポート グループ管理)*『*117*p. 』」を参照してください。
Dell® PowerEdge™ 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM (Other)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (Other)
IBM BladeCenter HT	IBM (Other)
IBM BladeCenter E	IBM BladeCenter E
HP®	ポート グループ管理機能を使用して設定します。「*HP および Cisco UCS のブレード シャーシ設定 (ポート グループ*

ブレード シャーシ モデル	KX III プロファイル
	管理)『*117*p. 』」を参照してください。

ブレード シャーシでサポートされている ***CIM***

以下の CIM は、KX III を通じて管理されるブレード シャーシでサポートされています。

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

以下の表に、KX III がサポートする各ブレード シャーシ モデルでサポートされている CIM を示します。

ブレード シャーシの場合	接続方法	推奨 CIM
Generic (汎用)	Generic (汎用) として設定されたブレード シャーシへの接続時に D2CIM-VUSB または D2CIM-DVUSB が使用されている場合は、[Port Configuration] (ポート設定) ページおよびクライアントの [USB Profile] (USB プロファイル) メニューから USB プロファイルを選択できます。ただし、汎用ブレード シャーシでは仮想メディアがサポートされないので、クライアントの [Virtual Media] メニューは無効になります。	• DCIM-PS2 • DCIM-USBG2
Cisco® UCS サーババシャーシ	Cisco KVM ケーブル (N20-BKVM) を使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、サーバ ブレードの管理、設定、および診断プロシージャを実行できます。 ソース: 『*Cisco UCS 5108 Server Chassis Installation Guide*』	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB

ブレード シャーシの場合	接続方法	推奨 CIM
Dell® PowerEdge™ 1855	以下の 3 つの KVM モジュールのいずれかを含みます。 • アナログ KVM Ethernet スイッチ モジュール (標準) • デジタル アクセス KVM スイッチ モジュール (オプション) • KVM スイッチ モジュール (2005 年 4 月以前に販売されたシステムでの標準) これらのスイッチは、2 つの PS/2 および 1 つのビデオ デバイスをシステムに接続できるカスタム コネクタを提供します。 ソース: *Dell PowerEdge 1855 システム ユーザーズ ガイド*	• DCIM-PS2
Dell PowerEdge 1955	2 種類の KVM モジュールのいずれかがインストールされる可能性があります。 • アナログ KVM スイッチ モジュール • デジタル アクセス KVM スイッチ モジュール どちらのモジュールでも、PS/2 互換のキーボード、マウス、およびビデオ モニタをシステムに接続できます (システムに付属のカスタム ケーブルを使用)。 ソース: *Dell PowerEdge 1955 ハードウェア オーナーズ マニュアル*	• DCIM-PS2
Dell PowerEdge M1000e	KVM スイッチ モジュール (iKVM) はこのシャーシに組み付けられています。 iKVM は、次の周辺機器に対応しています。 • USB キーボード、USB ポインティング デバイス • VGA モニタ (DDC サポート) ソース: *Dell Chassis Management Controller, Firmware Version 1.0, User Guide*	• DCIM-USBG2
HP® BladeSystem c3000	HP c-Class Blade SUV ケーブルを使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、ブレード シャーシの管理、設定、および診断プロシージャを実行できます。 ソース: HP Proliant™ BL480c Server Blade	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (KVM オプションを使用しない標準 KVM ポート操作の

ブレード シャーシの場合	接続方法	推奨 CIM
	Maintenance and Service Guide	場合)
HP BladeSystem c7000	HP c-Class Blade SUV ケーブルを使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、サーバ ブレードの管理、設定、および診断プロシージャを実行できます。 ソース: *HP ProLiant BL480c Server Blade Maintenance and Service Guide*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (標準 KVM ポート操作)
IBM® BladeCenter® S	Advanced Management Module (AMM) は、すべてのブレード シャーシのシステム管理機能およびキーボード/ビデオ/マウス (KVM) マルチプレキシングを提供します。 AMM 接続は、シリアル ポート、ビデオ接続、リモート管理ポート (Ethernet)、およびキーボードとマウス用の 2 つの USB v2.0 ポートが含まれます。 ソース: *Implementing the IBM BladeCenter S Chassis*	• DCIM-USBG2
IBM BladeCenter H	BladeCenter H シャーシには、アドバンスト マネージメント モジュールが 1 つ標準で付属しています。 ソース: *IBM BladeCenter Products and Technology*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	現在のモデル BladeCenter E シャーシ (8677-3Rx) には、アドバンスト マネージメント モジュールが 1 つ標準で属しています。 ソース: *IBM BladeCenter Products and Technology*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	BladeCenter T シャーシには、アドバンスト マネージメント モジュールが 1 つ標準で付属しています。 標準の BladeCenter シャーシとは異なり、BladeCenter T シャーシの KVM モジュールおよびマネージメント モジュールは、個別のコンポーネントになります。マネージメント モジュールの前面にあるのは、ステータスを表示する LED だけです。Ethernet および KVM 接続はすべて背面の LAN および KVM モジュ	• DCIM-PS2

ブレード シャーシの場合	接続方法	推奨 CIM
	ールで行います。 KVM モジュールは、ホット スワップ モジュールです。シャーシの背面にキーボードとマウス用の 2 つの PS/2 コネクタ、システム ステータス パネル、および HD-15 ビデオ コネクタがあります。 ソース: *IBM BladeCenter Products and Technology*	
IBM BladeCenter HT	BladeCenter HT シャーシには、アドバンスト マネージメント モジュールが 1 つ標準で付属しています。このモジュールは、シャーシを管理する機能とともに、ローカル KVM 機能も提供します。 ソース: *IBM BladeCenter Products and Technology*	• DCIM-USBG2

注: 自動検出をサポートするために、IBM BladeCenter モデル H および E では、ファームウェア バージョンが BPET36K 以降の AMM を使用する必要があります。

注: IBM Blade Center モデル E および H を使用する場合、KX III では、プライマリ管理モジュールとして AMM[1] の自動検出のみサポートされます。

注:音声は、すべての KVM スイッチ ターゲットで無効になります。

ブレード シャーシの必須および推奨設定

この表は、KX III で機能させるためのブレード シャーシの設定に適用される制限についての情報を示します。以下のすべての情報に従うことをお勧めします。

ブレード シャーシの場合	必須/推奨アクション
Dell® PowerEdge™ M1000e	▪ iKVM GUI スクリーンセーバを無効にします。無効にしていない場合は、認可のダイアログが表示され、iKVM が正しく機能しません。 ▪ Dell のシャーシを Raritan CIM に接続する前に iKVM GUI メニューを終了します。終了していない場合、iKVM が正しく動作しない場合があります。 ▪ iKVM GUI の［メイン］メニューを設定して、名前ではなくスロ

ブレード シャーシの場合	必須/推奨アクション
	ットでターゲット ブレードを選択します。この操作を行わない場合、iKVM は正しく機能しない可能性があります。 ▪ iKVM GUI の [設定] メニューの [スキャン] でスキャン操作にスロットを*指定しない*でください。指定した場合は iKVM が正しく機能しません。 ▪ iKVM GUI の [設定] メニューの [ブロードキャスト] でキーボード/マウスのブロードキャスト操作にスロットを*指定しない*でください。指定した場合は iKVM が正しく機能しません。 ▪ iKVM GUI を呼び出す 1 つのキー シーケンスを指定します。このキー シーケンスを、KX III でポートを設定するときにも指定する必要があります。そうしないと、クライアントのキー入力の結果として、iKVM 操作が無差別に発生する可能性があります。 ▪ Dell の CMC GUI を通じて iKVM を設定する際に、[フロント パネル USB/ビデオ有効] が*オフ*になっていることを確認します。オンになっている場合、シャーシの前面パネルでの接続が、背面の KX III 接続よりも優先されるので、適切な iKVM 処理が行われなくなります。"User has been disabled as front panel is currently active" (フロント パネルが現在アクティブになっているのでユーザは無効です) というメッセージが表示されます。 ▪ Dell の CMC GUI を通じて iKVM を設定する際に、[iKVM から CMC CLI へのアクセスを許可する] が*オフ*になっていることを確認します。 ▪ ブレード シャーシに接続するときに iKVM GUI が表示されないようにするには、[画面遅延時間] を 8 秒に設定します。 ▪ iKVM GUI のフラグ設定中に、[時間指定] および [表示] を選択することをお勧めします。これで、目的のブレード スロットとの接続を視覚的に確認できます。
Dell PowerEdge 1855/1955	▪ iKVM GUI スクリーンセーバを無効にします。これを行わない場合は [Authorize] (認可) ダイアログ ボックスが表示され、iKVM が正しく機能しなくなります。 ▪ Dell のシャーシを Raritan CIM に接続する前に iKVM GUI メニューを終了します。終了していない場合、iKVM が正しく動作しない場合があります。 ▪ iKVM GUI の [メイン] メニューを設定して、名前ではなくスロットでターゲット ブレードを選択します。この操作を行わない場合、iKVM は正しく機能しない可能性があります。 ▪ iKVM GUI の [設定] メニューの [スキャン] でスキャン操作にスロットを*指定しない*でください。指定した場合は iKVM が正しく機能しません。 ▪ ブレード シャーシに接続するときに iKVM GUI が表示されな

ブレード シャーシの場合	必須/推奨アクション
	いようにするには、[画面遅延時間] を 8 秒に設定します。 ▪ iKVM GUI のフラグ設定中に、[時間指定] および [表示] を選択することをお勧めします。これで、目的のブレード スロットとの接続を視覚的に確認できます。
IBM®/Dell® 自動検出	▪ ブレード レベルのアクセス許可を適用する場合は、自動検出を有効にすることをお勧めします。有効にしない場合は、ブレード シャーシ全体でのアクセス許可を設定します。 ▪ ブレード シャーシ管理モジュールで、Secure Shell (SSH) を有効にする必要があります。 ▪ ブレード シャーシ管理モジュールで設定された SSH ポートと、[Port Configuration] (ポート設定) ページで入力されるポート番号が一致する必要があります。
IBM KX3 仮想メディア	▪ Raritan KX III 仮想メディアは、IBM BladeCenter® モデル H および E でのみサポートされます。これは、D2CIM-DVUSB を使用する必要があります。黒の D2CIM-DVUSB 低速 USB コネクタは、本体背面の Administrative Management Module (AMM) に取り付けられます。グレーの D2CIM-DVUSB 高速 USB コネクタは、本体前面のメディア トレイ (MT) に取り付けられます。これには、USB 延長ケーブルが必要です。
Cisco® UCS サーバ シャーシ	▪ Cisco KVM ケーブル (N20-BKVM) を使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、サーバ ブレードの管理、設定、および診断プロシージャを実行できます。 ▪ ソース: *Cisco UCS 5108 Server Chassis Installation Guide* *(DCIM-USBG2、D2CIM-VUSB、D2CIM-DVUSB)*

注:AMM を使用するすべての IBM BladeCenter では、KX III で動作する AMM ファームウェア バージョン BPET36K 以降を使用する必要があります。

注: IBM Blade Center モデル E および H を使用する場合、KX III では、プライマリ管理モジュールとして AMM[1] の自動検出のみサポートされます。

ブレード シャーシのサンプル URL フォーマット

この表には、KX III で設定されるブレード シャーシのサンプル URL フォーマットが示されます。

ブレード シャーシの場合	サンプル URL フォーマット
Dell® M1000e	• URL: https://192.168.60.44/cgi-bin/webcgi/login

ブレード シャーシの場合	サンプル URL フォーマット
	• ユーザ名: root • ユーザ名フィールド: user • Password:calvin • パスワード フィールド: password
Dell 1855	• URL: https://192.168.60.33/Forms/f_login • ユーザ名: root • ユーザ名フィールド: TEXT_USER_NAME • Password:calvin • パスワード フィールド: TEXT_PASSWORD
IBM® BladeCenter® E または H	• http://192.168.84.217/private/welcome.ssi

USB プロファイルの設定 ([Port] (ポート) ページ)

ポートで使用できる USB プロファイルを、[Port] (ポート) ページの [Select USB Profiles for Port] (ポートの USB プロファイルの選択) セクションで選択します。[Port] (ポート) ページで選択された USB プロファイルが、ポートから KVM ターゲット サーバに接続するときに VKC でユーザが使用できるプロファイルになります。デフォルト値は、Windows 2000®/Windows XP®/Windows Vista® 用のプロファイルです。USB プロファイルについての詳細は、「USB プロファイル」を参照してください。

---

*注:ポートの USB プロファイルを設定するには、デジタル CIM、VM-CIM、またはデュアル VM-CIM を、KX III の現在のファームウェア バージョンと互換性のあるファームウェアに接続しておく必要があります。「***CIM をアップグレードする*** *『196p. の*"***CIM アップグレード***"*参照 』」を参照してください。*

ポートへの割り当てに使用できるプロファイルは、左側の [Available] (使用可能) リストに表示されます。ポートで使用するように選択したプロファイルは、右側の [Selected] (選択) リストに表示されます。いずれかのリストでプロファイルを選択した場合、プロファイルとその使用についての説明が [Profile Description] (プロファイルの説明) フィールドに表示されます。

KVM ポートで使用可能にする一連のプロファイルを選択する他に、ポートの優先プロファイルを指定して、あるポートに対する設定を他の KVM ポートに適用することもできます。

---

*注:DCIM-VUSB または DCIM-DVUSB 仮想メディア CIM を使用している場合、Mac OS-X® USB プロファイルの使用法については、「***Mac のブート メニュー使用時のマウス モード*** *『56p. 』」を参照してください。*

▶ **[Port] (ポート) ページを開くには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。
2. 編集する KVM ポートの [Port Name] (ポート名) をクリックします。[Port] (ポート) ページが開きます。

▶ **KVM ポートの USB ポートを選択するには、以下の手順に従います。**

1. [Select USB Profiles for Port] (ポートの USB プロファイルの選択) セクションで、1 つ以上の USB プロファイルを [Available] (使用可能) リストから選択します。
   - Shift キーを押しながらクリックしてドラッグすると、複数の隣接するプロファイルを選択できます。
   - Ctrl キーを押しながらクリックすると、隣接していない複数のプロファイルを選択できます。

2. [Add] (追加) をクリックします。選択したプロファイルが [Selected] (選択) リストに表示されます。これらは、ポートに接続された KVM ターゲット サーバで使用できるプロファイルです。

▶ 優先 USB プロファイルを指定するには、以下の手順に従います。

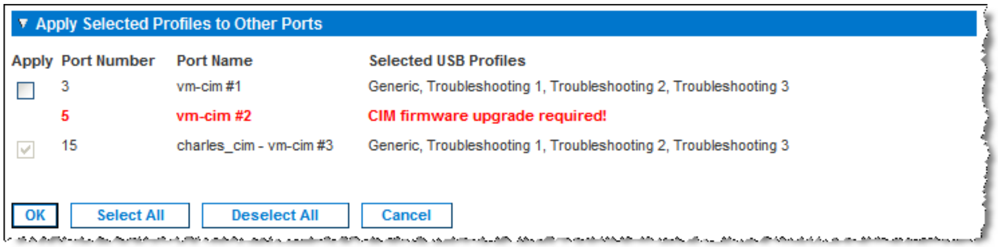
1. ポートで使用可能なプロファイルを選択した後、[Port] (ポート) メニューの [Preferred Profile] (優先プロファイル) から 1 つを選択します。デフォルトは [Generic] (汎用) です。選択したプロファイルは、KVM ターゲット サーバに接続するときに使用されます。必要に応じて、他の USB プロファイルに変更できます。
2. [Set Active Profile As Preferred Profile] (アクティブ プロファイルを優先プロファイルとして設定) チェックボックスをオンにすると、この優先 USB もアクティブ プロファイルとして使用されます。

▶ 選択した USB プロファイルを削除するには、以下の手順に従います。

1. [Select USB Profiles for Port] (ポートの USB プロファイルの選択) セクションで、1 つ以上の USB プロファイルを [Selected] (選択) リストから選択します。
   - Shift キーを押しながらクリックしてドラッグすると、複数の隣接するプロファイルを選択できます。
   - Ctrl キーを押しながらクリックすると、隣接していない複数のプロファイルを選択できます。
2. [Remove] (削除) をクリックします。選択したプロファイルが [Available] (使用可能) リストに表示されます。これらのプロファイルは、このポートに接続された KVM ターゲット サーバでは使用できなくなります。

▶ プロファイルの選択を複数のポートに適用するには、以下の手順に従います。

1. [Apply Selected Profiles to Other Ports] (選択したプロファイルを他のポートに適用) セクションで、選択した USB プロファイルの現在の設定を適用する各 KVM ポートの [Apply] (適用) チェックボックスをオンにします。



   - すべての KVM ポートを選択するには、[Select All] (すべて選択) をクリックします。

- すべての KVM ポートの選択を解除するには、[Deselect All] (すべての選択を解除) をクリックします。

KX III ローカル ポートの設定

注:[Local Port Settings] (ローカル ポート設定) ページで設定を変更すると、作業中のブラウザが再起動する場合があります。変更時にブラウザが再起動する設定については、以下の手順に示されています。

ローカル ポートに関する設定値をカスタマイズするには

- [Device Settings] (デバイス設定) メニューの [Local Port Settings] (ローカル ポート設定) をクリックします。[Local Port Settings] (ローカル ポート設定) ページが開きます。

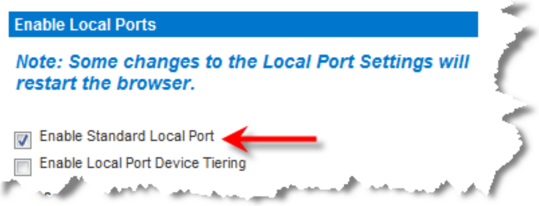
標準ローカル ポートの有効化

1. 標準ローカル ポートを有効にするには、[Enable Standard Local Port] (標準ローカル ポートを有効にする] チェック ボックスをオンにします。無効にするにはチェックボックスをオフにします。

   デフォルトでは、標準ローカル ポートは有効になっていますが、必要に応じて無効にすることができます。

   この設定を変更すると、ブラウザが再起動します。

   注:カスケード接続機能を利用する場合は、標準ローカル ポート機能は無効になります。両方の機能を同時に利用できないためです。

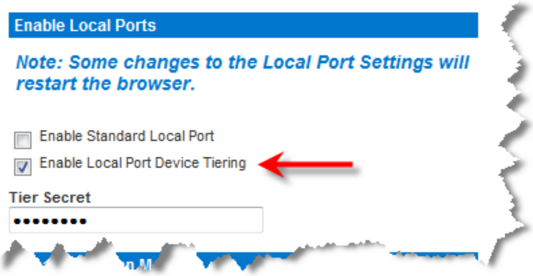


ローカル ポート デバイスのカスケード接続の有効化

1. カスケード接続機能を利用する場合、[Enable Local Port Device Tiering] (ローカル ポート デバイスのカスケード接続を有効にする] チェック ボックスをオンにし、[Tier Secret] (カスケード接続秘密ワード) フィールドにカスケード接続秘密ワードを入力します。

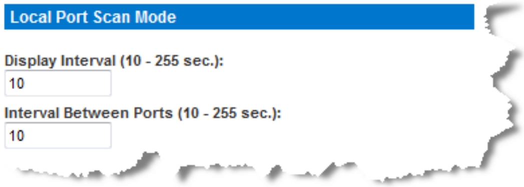
   カスケード接続を設定するには、[Device Services] (デバイス サービス) ページでベース デバイスを設定する必要があります。

カスケード接続の詳細については、「カスケード接続を設定および有効化する」を参照してください。



ローカル ポート スキャン モードの設定

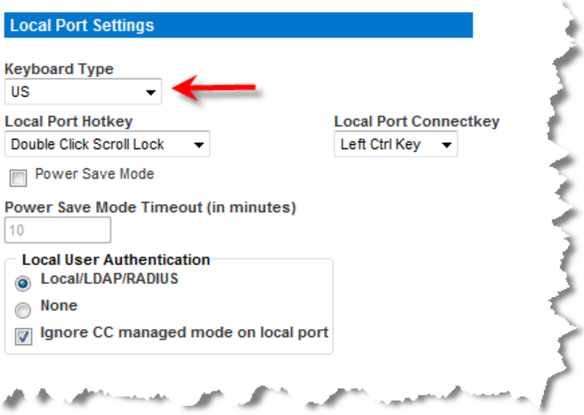
1. 必要な場合は、[ローカル ポート スキャン モード] 設定をカスタマイズします。これらの設定は、[ポート] ページからアクセスされるスキャン設定機能に適用されます。「ポートのスキャン」を参照してください。
   - [表示間隔 (10 ～ 255 秒):]: フィールドで、フォーカスを持つターゲットを [ポート スキャン] ウィンドウの中央に表示する秒数を指定します。
   - [ポート間の間隔 (10 ～ 255 秒):] フィールドで、ポート間でデバイスを一時停止する間隔を指定します。



ローカル コンソールのキーボード タイプの選択

1. [Keyboard Type] (キーボード タイプ) ドロップダウン リストでキーボード タイプを選択します。選択できる項目は次のとおりです。

   この設定を変更すると、ブラウザが再起動します。



- [US] (アメリカ英語)
- [US/International] (アメリカ英語/国際)
- [United Kingdom] (イギリス英語)
- [French (France)] (フランス語 (フランス))
- [German (Germany)] (ドイツ語 (ドイツ))
- [German (Switzerland)] (ドイツ語 (スイス))
- [Simplified Chinese] (簡体字中国語)
- [Traditional Chinese] (繁体字中国語)
- [Dubeolsik Hangul (Korean)] (Dubeolsik ハングル (韓国))
- [JIS (Japanese Industry Standard)] (JIS (日本工業規格))
- [Portuguese (Portugal)] (ポルトガル語 (ポルトガル))
- [Norwegian (Norway)] (ノルウェー語 (ノルウェー))
- [Swedish (Sweden)] (スウェーデン語 (スウェーデン))
- [Danish (Denmark)] (デンマーク語 (デンマーク))
- [Belgian (Belgium)] (ベルギー語 (ベルギー))
- ハンガリー語
- スペイン語
- イタリア語
- スロベニア語

注:中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。

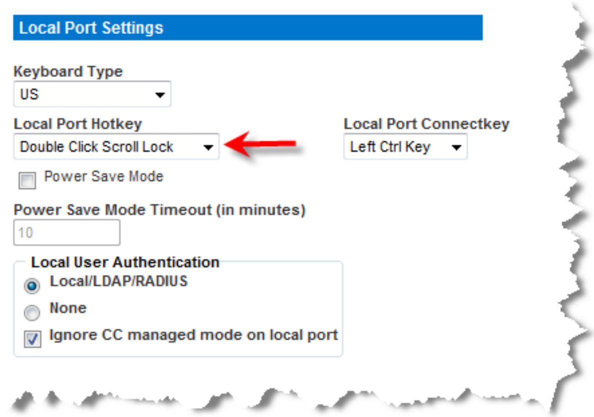
注:トルコ語のキーボードを使用している場合は、Active KVM Client (AKC) を介してターゲット サーバに接続する必要があります。他の Raritan クライアントではサポートされていません。

ローカル ポート ホットキーの選択

1. [Local Port Hotkey] (ローカル ポート ホットキー) ボックスの一覧でローカル ポート ホットキーを選択します。ローカル ポート ホットキーは、ターゲット サーバの画面が表示されているときに KX III ローカル コンソールの画面に戻す際に使用します。デフォルト値は [Double Click Scroll Lock] (Scroll Lock キーを 2 回押す) ですが、他のキー組み合わせを選択することもできます。

ホットキー	説明
Scroll Lock キーをすばやく 2 回押す	Scroll Lock キーをすばやく 2 回押します。
[Double Click Num Lock] (Num Lock キーを 2 回押す)	Num Lock キーをすばやく 2 回押します。
[Double Click Caps Lock]	Caps Lock キーをすばやく 2 回押し

ホットキー	説明
(Caps Lock キーを 2 回押す)	ます。
[Double Click Left Alt key] (左 Alt キーを 2 回押す)	左 Alt キーをすばやく 2 回押します。
[Double Click Left Shift key] (左 Shift キーを 2 回押す)	左 Shift キーをすばやく 2 回押します。
[Double Click Left Ctrl key] (左 Ctrl キーを 2 回押す)	左 Ctrl キーをすばやく 2 回押します。



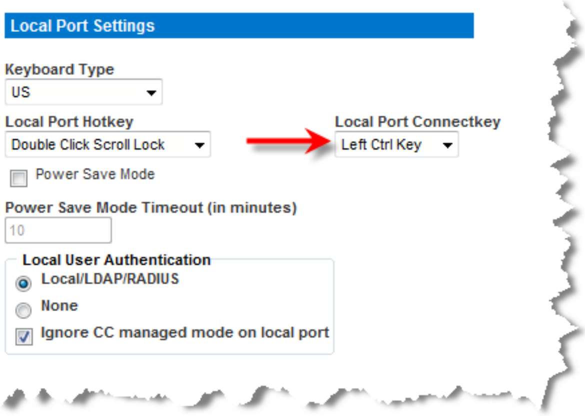
ローカル ポート接続キーの選択

1. ローカル ポート接続キーを選択します。接続キーは、あるターゲット サーバにアクセスしているときに別のターゲット サーバに切り替える際に使用します。

   その後ホットキーを使用して、そのターゲット サーバの画面から KX III ローカル コンソールの画面に戻すことができます。

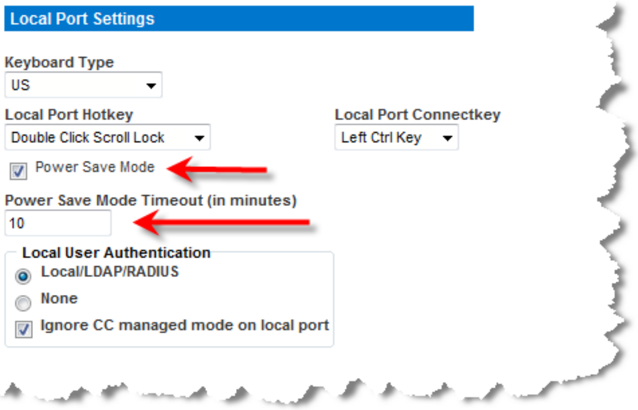
   接続キーを設定すると、ナビゲーション パネルに表示されるので、すぐにわかります。接続キー組み合わせの例については、「***接続キーの例*** 『*299*p. 』」を参照してください。

接続キーは、標準型サーバとブレード筐体のどちらに対しても機能します。



省電力機能の設定 (オプション)

1. 省電力機能を利用する場合、次の手順を実行します。
   a. [Power Save Mode] (省電力モード) チェック ボックスをオンにします。
   b. [Power Save Mode Timeout (in minutes)] (省電力モードのタイムアウト (分)) ボックスに、省電力モードに移行するまでの時間 (単位: 分) を入力します。

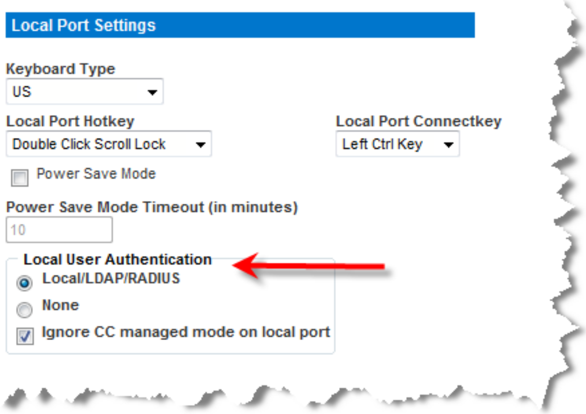


ローカル ユーザ認証の選択

1. [Local User Authentication] (ローカル ユーザ認証) でローカル ユーザ認証タイプを選択します。
   - [Local/LDAP/RADIUS] (ローカル/LDAP/RADIUS)これは推奨オプションです。

     認証の詳細については、「リモート認証」を参照してください。
   - 特別なアクセス用ソフトウェアをインストールする必要はありません。KX III ローカル コンソールからのアクセスに対して認証は行われません。

このオプションは、安全な環境でのみ選択することを推奨します。



[Device Services] (デバイス サービス)

SSH を有効にする

管理者が SSH v2 アプリケーションを使用して KX III にアクセスできるようにするには、[Enable SSH Access] (SSH アクセスを有効にする) チェック ボックスをオンにします。

▶ SSH アクセスを有効にするには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Enable SSH Access] (SSH アクセスを有効にする) を選択します。
3. [SSH Port Information] (SSH ポート情報) を入力します。標準の SSH TCP ポート番号は 22 ですが、ポート番号を変更して高いレベルのセキュリティ処理を提供することもできます。
4. [OK] (OK) をクリックします。

HTTP ポートおよび HTTPS ポートの設定

KX III によって使用される HTTP ポートまたは HTTPS ポートを設定できるようになりました。 たとえば、デフォルトの HTTP ポートであるポート 80 を別の用途で使用している場合、HTTP 用ポートを変更すると、ポート 80 が HTTP 用として使用されなくなります。

▶ HTTP ポートまたは HTTPS ポートの設定を変更するには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。

2. [HTTP Port] (HTTP ポート) フィールドまたは [HTTPS Port] (HTTPS ポート) フィールド (あるいはその両方) に新しいポート番号を入力します。
3. [OK] (OK) をクリックします。

検出ポートを入力する

KX III の検出は、設定可能な 1 つの TCP ポートで行われます。デフォルトではポート 5000 に設定されていますが、80 と 443 以外であれば、どの TCP ポートを使用するよう設定してもかまいません。ファイアウォールの外側から KX III にアクセスするには、お使いのファイアウォールの設定で、デフォルト ポート 5000 または上記で設定したデフォルト以外のポートを使用する双方向通信を有効にする必要があります。

▶ 検出ポートを有効にするには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Discovery Port] (検出ポート) を入力します。
3. [OK] (OK) をクリックします。

カスケード接続を設定および有効化する

カスケード接続機能を利用した場合、1 台のベース KX III デバイスを介して KX III ターゲットと PDU にアクセスできます。

必要に応じて、カスケード接続構成にデバイスを追加することやカスケード接続構成からデバイスを削除することができます。カスケード接続レベルは最大 2 段階です。

デバイスをセットアップする際、特定のカスケード接続構成に対して特定の CIM を使用します。

カスケード接続構成に追加できるターゲット、CIM の互換性、およびデバイス設定情報については、「カスケード接続: ターゲット タイプ、サポート対象 CIM、およびカスケード接続構成」を参照してください。

CIM 名の変更などのポート設定は、各デバイスから直接行う必要があります。カスケード接続ターゲット ポートの設定は、ベース デバイスから行うことはできません。

カスケード接続構成では、KVM スイッチを使用してサーバを切り替えることもできます。「*KVM スイッチを設定する* 『*93*p. 』」を参照してください。

設定したら、ベース デバイスおよびカスケード接続デバイスが [Port Access] (ポート アクセス) ページで表示されます。「*カスケード接続デバイス - [Port Access] (ポート アクセス) ページ* 『*18*p. 』」を参照してください。

カスケード接続を構成する前に

カスケード接続を構成する前に、「***許可されている KX III カスケード接続構成***『*136*p. 』」および「カスケード接続ターゲットでサポートされていない機能および限定的にサポートされている機能」を確認してください。

KX III カスケード構成にカスケード接続デバイスを追加する前に、以下が求められます。

- ベース デバイスおよびカスケード接続デバイスはすべて同じファームウェア リビジョンで動作している必要があります。
- ベース デバイスでカスケード接続を有効にするには、[Device Settings] (デバイス設定) ページを使用します。「標準ターゲット サーバの設定」を参照してください。
- カスケード接続デバイスでカスケード接続を有効にするには、[Local Port Settings] (ローカル ポート設定) ページを使用します。「***KX III ローカル ポートの設定***『*129*p. 』」、「***ローカル ポート デバイスのカスケード接続の有効化***『*129*p. 』」の順に参照してください。
- ベースデバイスのカスケード接続を有効にし、次にカスケード接続デバイスを有効にします。「***カスケード接続を有効にする***『*138*p. 』」を参照してください。

*許可されている **KX III** カスケード接続構成*

デバイスをカスケード接続する前に、「***カスケード接続を構成する前に***『*136*p. 』」を確認してください。

KX III の許可されているカスケード接続構成を以下に示します。

- KX III ベース デバイス > KX III カスケード接続デバイス
- KX III ベース デバイス > KX II カスケード接続デバイス
- カスケード接続デバイスに接続されたデュアル ビデオ ポート ターゲットには、カスケード接続デバイスを介して接続する必要があります。

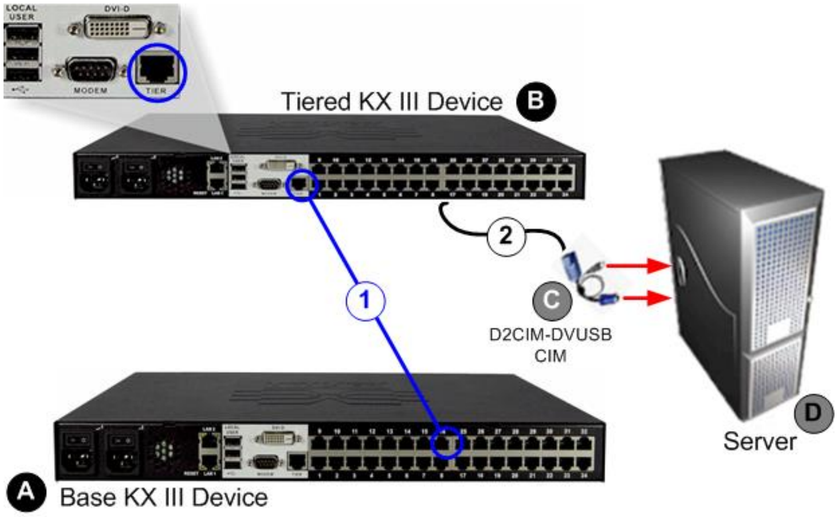
カスケード接続ターゲットでサポートされていない機能および限定的にサポートされている機能

カスケード接続ターゲットでサポートされていない機能は次のとおりです。

- ブレード シャーシ
- 音声
- カスケード接続デバイスでのスマート カード
- 仮想メディア
- MCCAT
- ポート グループ管理機能に制限があり、ベース デバイスに直接接続されているメンバーのポート グループしか作成できません。
- カスケード接続デバイスに接続されたデュアル ビデオ ポート ターゲットには、カスケード接続ベース デバイスを介して接続しないでください。
- KX III と KX II が混在するカスケード接続構成では、ずれないマウス機能は正しく同期しない場合があります。
- KX II ベース デバイス ＞KX III カスケード接続デバイス

KX III のカスケード接続例

次の図に、カスケード接続 KX III デバイスとベース KX III デバイスの接続例を示します。



手順	
A	KX III ベース デバイス
B	KX III カスケード接続デバイス
C	ターゲット サーバを KX III カスケード接続デバイスに接続するための CIM
D	ターゲット サーバ
1	ベース デバイスのカスケード接続ポートからカスケード接続デバイスのカスケード接続ポートへの接続 ▪ Cat5/5e/6 ケーブルの片側を KX III ベース デバイスのターゲット サーバ ポートに接続します。 ▪ このケーブルの反対側を KX III カスケード接続デバイスのカスケード接続ポートに接続します。
2	ターゲット サーバのキーボード/ビデオ/マウス ポートへのカスケード接続デバイスの接続: ▪ Cat5/5e/6 ケーブルの片側を KX III カスケード接続デバイスのターゲット サーバ ポートに接続し、反対側を D2CIM-DVUSB のようなサポートされている CIM に接続します。 ▪ CIM のキーボード、マウス、ビデオの各プラグをターゲット サーバの対応するポートに接続します。

カスケード接続を有効にする

▶ カスケード接続を有効にするには

1. カスケード接続ベース デバイスで、[Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択して、[Device Service Settings] (デバイス サービス設定) ページを開きます。
2. [Enable Tiering as Base] (ベースとしてのカスケード接続を有効にする) を選択します。
3. [Base Secret] (ベース秘密ワード) フィールドに、ベース デバイスとカスケード接続デバイスの間で共有される秘密ワードを入力します。この秘密ワードは、カスケード接続デバイスでベース デバイスを認証する際に必要となります。同じ秘密ワードをカスケード接続デバイスに対して入力します。[OK] をクリックします。

Raritan.

4. カスケード接続デバイスを有効にします。カスケード接続デバイスで、[Device Settings] (デバイス設定) の [Local Port Settings] (ローカル ポート設定) を選択します。
5. このページの [Enable Local Ports] (ローカル ポートを有効にする) セクションで、[Enable Local Port Device Tiering] (ローカル ポート デバイスのカスケード接続を有効にする) を選択します。
6. [Tier Secret] (カスケード接続秘密ワード) フィールドに、ベース デバイスの [Device Settings] (デバイス設定) ページで入力したのと同じ秘密ワードを入力します。[OK] をクリックします。

デバイスに対してカスケード接続を有効化および設定すると、そのデバイスが [Port Access] (ポート アクセス) ページに表示されます。

KX III をベース デバイスまたはカスケード接続デバイスとして機能するように設定すると、そのデバイスは次のように表示されます。

- ベース デバイスとして設定した場合、KX III 画面の左パネルの [Device Information] (デバイス情報) セクションに、[Configured As Base Device] (ベース デバイスとして設定) と表示されます。
- カスケード接続デバイスとして設定した場合、KX III 画面の左パネルの [Device Information] (デバイス情報) セクションに、[Configured As Tier Device] (カスケード接続デバイスとして設定) と表示されます。
- ベース デバイスは、カスケード接続デバイスの画面の左パネルの [Connect User] (接続しているユーザ) の下で [Base] (ベース) として表示されます。
- ベース デバイスのカスケード接続ポートに接続しているターゲットは、2 つのポートに接続しているように表示されます。

カスケード接続デバイスからのリモート アクセスとローカル アクセス

ベース デバイスからは、[Port Access] (ポート アクセス) ページに表示されている統合ポート リストを使用して、リモート アクセスおよびローカル アクセスできます。

カスケード接続デバイスからは、そのデバイスのポート リストを使用してリモート アクセスできます。

カスケード接続が有効になっている場合、カスケード接続デバイスからローカル アクセスすることはできません。

ベース デバイスからブレード シャーシへのアクセス

KX III ベース デバイスに直接接続されているブレード シャーシにアクセスできます。

カスケード接続デバイスからの電源制御

カスケード接続構成に含まれているターゲットの電源を入れたり切ったりできます。

これらのターゲットにアクセスするには、[Port Access] (ポート アクセス) ページを使用します。

ターゲットとコンセントが関連付けられている場合、[Port Access] (ポート アクセス) ページで電源を制御できます。

ターゲットと PDU コンセントを関連付けることができるのは、両者が同じ KX III に接続されている場合だけです。

ベース KX III またはカスケード接続 KX III に接続されている PDU は、[Power] (電源) ページのドロップダウン リストに表示されます。電源タップを選択すると、その統計情報が表示されます。

コンセント レベルも制御できます。

具体的には、現在オンになっているコンセントをオフにすることができますが、現在オフになっているコンセントをオンにすることはできません。

URL を経由したダイレクト ポート アクセスの有効化

ダイレクト ポート アクセス機能を利用した場合、ユーザはデバイスの [Login] (ログイン) ダイアログ ボックスと [Port Access] (ポート アクセス) ページを使用する必要がなくなります。

この機能を使用すると、ユーザ名とパスワードが URL に含まれていない場合に、ユーザ名とパスワードを直接入力してターゲットにアクセスすることもできます。

Virtual KVM Client (VKC) のダイレクト ポート アクセス URL 構文

Virtual KVM Client (VKC) とダイレクト ポート アクセスを使用する場合は、次の標準ポートの構文のいずれかを使用してください。

- https://IPaddress/dpa.asp?username=username&password=password&port=port number

  または

- https://IPaddress/dpa.asp?username=username&password=password&portname=port name

ブレード シャーシについては、ポートをポート番号またはポート名、およびスロット番号の両方で指定する必要があります。

- https://IPaddress/dpa.asp?username=username&password=password&port=port number-slot number

  たとえば、ブレード シャーシがポート 1、スロット 2 に接続されている場合、port number-slot number には 1-2 を指定します。

- https://IPaddress/dpa.asp?username=username&password=password&port=port name-slot number

  たとえば、ブレード シャーシがポート 1、スロット 2 に接続されている場合、port name-slot number には Port1-2 を指定します。

username と password はオプションです。

ユーザ名とパスワードを指定しない場合は、ログイン ダイアログ ボックスが表示され、認証後、ユーザはターゲットに直接接続されます。

port には、ポート番号またはポート名を指定できます。

ポート名を使用する場合は、一意の名前にしなければ、エラーが報告されます。

port を省略した場合もエラーが報告されます。

デュアル ポート ビデオ グループに属しているターゲットにアクセスする場合は、ダイレクト ポート アクセスにより、プライマリポートを使用して、プライマリ ポートおよびセカンダリ ポートの両方を開きます。

セカンダリ ポートへのダイレクト ポート接続は拒否され、通常の権限ルールが適用されます。

デュアル ポート ビデオ グループ機能については、「**デュアル ビデオ ポート グループの作成** 『166p. 』」を参照してください。 。

Active KVM Client (AKC) のダイレクト ポート アクセス URL 構文

Active KVM Client (AKC) とダイレクト ポート アクセスを使用する場合は、:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=akc

  または

- https://IPaddress/dpa.asp?username=username&password=password&port=port name&client=akc

ブレード シャーシについては、ポートをポート番号またはポート名、およびスロット番号の両方で指定する必要があります。

- https://IPaddress/dpa.asp?username=username&password=password&port=port number-slot number=akc

  たとえば、ブレード シャーシがポート 1、スロット 2 に接続されている場合、port number-slot number には 1-2 を指定します。

- https://IPaddress/dpa.asp?username=username&password=password&port=port name-slot number=akc

  たとえば、ブレード シャーシがポート 1、スロット 2 に接続されている場合、port name-slot number には Port1-2 を指定します。

username と password はオプションです。

ユーザ名とパスワードを指定しない場合は、ログイン ダイアログ ボックスが表示され、認証後、ユーザはターゲットに直接接続されます。

port には、ポート番号またはポート名を指定できます。

ポート名を使用する場合は、一意の名前にしなければ、エラーが報告されます。

port を省略した場合もエラーが報告されます。

client=akc は、AKC クライアントを使用しない場合はオプションです。

client=akc を指定しない場合は、Virtual KVM Client (VKC) がクライアントとして使用されます。

デュアル ポート ビデオ グループに属しているターゲットにアクセスする場合は、ダイレクト ポート アクセスにより、プライマリポートを使用して、プライマリ ポートおよびセカンダリ ポートの両方を開きます。

セカンダリ ポートへのダイレクト ポート接続は拒否され、通常の権限ルールが適用されます。

デュアル ポート ビデオ グループ機能については、「**デュアル ビデオ ポート グループの作成** 『166p. 』」を参照してください。 。

ダイレクト ポート アクセスの有効化

▶ ダイレクト ポート アクセスを有効するには、以下の手順に従います。

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. URL で必要なパラメータを渡してユーザに Dominion デバイス経由でターゲットに直接アクセスさせる場合は、[Enable Direct Port Access via URL] (URL を介したダイレクト ポート アクセスを有効にする) を選択します。
3. [OK] をクリックします。

AKC ダウンロード サーバ証明書の検証の有効化

AKC クライアントを使用する場合は、[Enable AKC Download Server Certificate Validation (AKC ダウンロード サーバ証明書の検証を有効にする)] 機能を使用するかどうかを選択できます。

注:[Enable AKC Download Server Certificate Validation] (AKC ダウンロード サーバ証明書の検証を有効にする) 機能と共に IPv4 および IPv6 デュアル スタック モードで動作している場合、Microsoft® ClickOnce® では、サーバ証明書 CN に IPv6 アドレスのゼロ圧縮形式を含めてはなりません。

ゼロ圧縮形式を含めると、AKC を正常にダウンロードして起動することができなくなります。

ただし、これは IPv6 アドレスの形式に対するブラウザの設定と競合する場合があります。

共通名 (CN) でサーバのホスト名を使用するか、証明書の「サブジェクトの別名」に IPv6 アドレスの圧縮形式や非圧縮形式を含めてください。

オプション 1: AKC ダウンロード サーバ証明書の検証を有効にしない (デフォルト設定)

AKC ダウンロード サーバ証明書の検証を有効にしない場合は、以下の操作を行います。すべての Dominion デバイス ユーザおよび CC-SG Bookmark and Access Client ユーザは、次のことを行う必要があります。

- アクセスするデバイスの IP アドレスからの Cookie が現在ブロックされていないことを確認します。
- Windows Vista、Windows 7、および Windows 2008 Server のユーザは、アクセスするデバイスの IP アドレスがブラウザの [信頼済みサイト] ゾーンに含まれ、デバイスへのアクセス時に保護モードが有効になっていないことを確認する必要があります。

オプション 2: AKC ダウンロード サーバ証明書の検証を有効にする

AKC ダウンロード サーバ証明書の検証を有効にする場合は、以下の操作を行います。

- 管理者は、有効な証明書をデバイスにアップロードするか、自己署名証明書をデバイスで生成する必要があります。証明書で有効なホストが指定されている必要があります。
- 各ユーザは、CA 証明書 (または自己署名証明書のコピー) をブラウザの信頼されたルート証明機関ストアに追加する必要があります。
- CC-SG ネイバーフッドを使用する場合は、各ネイバーフッド メンバーの AKC を有効にする必要があります。

▶ **Windows Vista® または Windows 7® オペレーティング システムを使用している場合、自己署名証明書をインストールするには、以下の手順に従います。**

1. [信頼済みサイト] ゾーンに KX III の IP アドレスを追加し、保護モードがオフになっていることを確認します。
2. URL に KX III の IP アドレスを使用して Internet Explorer® を起動します。証明書エラー メッセージが表示されます。
3. [証明書の表示] を選択します。
4. [全般] タブで、[証明書のインストール] をクリックします。証明書が信頼されたルート証明機関ストアにインストールされます。
5. 証明書のインストール後、KX III の IP アドレスを [Trusted Site (信頼済みサイト)] ゾーンから削除する必要があります。

▶ AKC ダウンロード サーバ証明書の検証を有効にするには、以下の手順に従います。

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Enable AKC Download Server Certificate Validation (AKC ダウンロード サーバ証明書の検証を有効にする)] チェックボックスをオンにするか、この機能を無効 (デフォルト) のままにしておくことができます。
3. [OK] をクリックします。

If you are connecting to a KX III standalone device and support for AKC download server certificate validation is enabled, the valid IPv6 format to generate the certificate is either:

- `CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]` when there is a leading 0

  or

- `CN =[fd07:02fa:6cff:2500:020d:5dff:0000:01c0]` when there is no zero compression

SNMP エージェントの設定

SNMP に準拠したデバイスはエージェントと呼ばれます。それ自体のデータは Management Information Base (MIB) に格納され、デバイスはそのデータを SNMP マネージャに返します。KX III の MIB の表示方法については、「*KX III の MIB の表示* 『*154*p. 』」を参照してください。

KX III は、SNMP v1/v2c や v3 の SNMP ログをサポートします。SNMP ログが有効になっている場合は、SNMP v1/v2c で、メッセージ形式およびプロトコル操作が定義されます。SNMP v3 は SNMP のセキュリティを拡張したものであり、ユーザ認証、パスワード管理、および暗号化を提供します。

► **SNMP エージェントを設定するには、以下の手順に従います。**

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. MIB-II システム グループ オブジェクトに次の SNMP エージェント識別子情報を設定します。
   a. System Name - SNMP エージェントの名前/デバイス名
   b. System Contact - デバイスに関連する連絡先名
   c. System Location - デバイスの場所
3. [Enable SNMP v1/v2c] (SNMP v1/v2c を有効にする) または [Enable SNMP v3] (SNMP v3 を有効にする) を選択するか、その両方を選択します。少なくとも 1 つのオプションを選択する必要があります。**必ず入力してください。**
4. SNMP v1/v2c 用の次のフィールドに入力します (必要な場合)。
   a. Community - デバイスのコミュニティ文字列
   b. Community Type - コミュニティ ユーザに読み取り専用または読み書き可能のアクセスを許可

   注:SNMP コミュニティとは、SNMP を実行しているデバイスと管理ステーションが所属するグループのことです。SNMP コミュニティは、情報の送信先を定義するのに役立ちます。コミュニティ名は、グループを識別するために使用されます。SNMP デバイスや SNMP エージェントは、複数の SNMP コミュニティに所属できます。

   ---
5. SNMP v3 用の次のフィールドに入力します (必要な場合)。
   a. 必要な場合は、[Use Auth Passphrase] (認証パスフレーズの使用) を選択します。プライバシー パスフレーズが必要な場合は、[Use Auth Passphrase] (認証パスフレーズの使用) により、認証パスフレーズを再入力しなくても、両方に同じパスフレーズを設定できます。

b. [Security Name] (セキュリティ名) – SNMP エージェントと通信するエンティティのユーザ名またはサービス アカウント名 (32 文字以内)

c. [Authentication Protocol] (認証プロトコル) – SNMP v3 エージェントで使用される MD5 または SHA 認証プロトコル

d. [Authentication Passphrase] (認証パスフレーズ) – SNMP v3 エージェントへのアクセスに必要なパスフレーズ (64 文字以内)

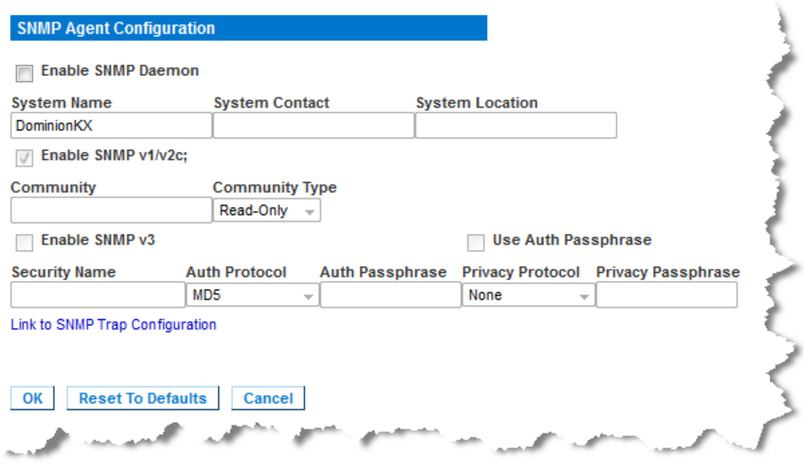
e. [Privacy Protocol] (プライバシー プロトコル) – 必要に応じて PDU やコンテキスト データの暗号化に使用される AES または DES アルゴリズム

f. [Privacy Passphrase] (プライバシー パスフレーズ) – プライバシー プロトコル アルゴリズムへのアクセスに使用されるパスフレーズ (64 文字以内)

6. [OK] をクリックすると、SNMP エージェント サービスが開始されます。

[Event Management – Settings] (イベント管理 – 設定) ページには、SNMP トラップ設定のリンクをクリックすると、すばやくアクセスできます。SNMP トラップの作成方法については、「*SNMP トラップの設定* 『*148*p. 』」を参照し、KX III の使用可能な SNMP トラップについては、「KX III SNMP トラップのリスト」を参照してください。

SNMP トラップを設定するとキャプチャされるイベントは、[Event Management – Destinations] (イベント管理 – 送信先) ページで選択されます。「*[Event Management – Destinations] (イベント管理 – 送信先) の設定* 『*156*p. 』」を参照してください。



▶ **工場出荷時のデフォルトに戻すには、以下の手順に従います。**

- [Reset to Defaults] (デフォルトに戻す) をクリックします。ページのすべての項目がデフォルト値に戻されます。

> 警告: UDP 経由の SNMP トラップを使用している場合は、KX III を再起動したときに KX III と接続先のルータが同期しなくなり、再起動完了の SNMP トラップがログ記録されなくなるおそれがあります。

モデムを設定する

注:リリース KX III 3.0.0 では、モデムがサポートされていませんが、今後のリリースでサポートされる予定です。

日付/時刻の設定

[Date/Time Settings] (日付/時刻の設定) ページを使用して、KX III の日付と時刻を指定します。これには 2 とおりの方法があります。

- 手動で日付と時刻を設定する。
- 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期する。

▶ **日付と時刻を設定するには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Date/Time] (日付/時刻) を選択します。[Date/Time Settings] (日付/時刻の設定) ページが開きます。
2. [Time Zone] (タイム ゾーン) ドロップダウン リストから適切なタイム ゾーンを選択します。
3. 夏時間用の調整を行うには、[Adjust for daylight savings time] (夏時間用の調整) チェックボックスをオンにします。
4. 日付と時刻の設定に用いる方法を選択します。
   - [User Specified Time] (ユーザによる時刻定義) – 日付と時刻を手動で入力する場合に、このオプションを使用します。[User Specified Time] (ユーザによる時刻定義) オプションを選択した場合は、日付と時刻を入力します。時刻は、hh:mm の形式を使用します (24 時間制で入力します)。
   - [Synchronize with NTP Server] (NTP サーバと同期) – 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期する場合に、このオプションを使用します。
5. [Synchronize with NTP Server] (NTP サーバと同期) オプションを選択した場合は、以下の手順に従います。
   a. [Primary Time server] (プライマリ タイム サーバ) の IP アドレスを入力します。

b. [Secondary Time server] (セカンダリ タイム サーバ) の IP アドレスを入力します。(オプション)

6. [OK] をクリックします。

イベント管理

KX III イベント管理機能によって、SNMP マネージャ、Syslog、監査ログへのシステム イベントの送信を有効または無効にできます。 これらのイベントはカテゴリ分けされるため、イベントごとに 1 つまたは複数の宛先に送信するかどうかを指定できます。

[Event Management - Settings] (イベント管理 - 設定) の設定

[Event Management - Settings] (イベント管理 - 設定) ページで SNMP トラップおよび syslog を設定します。「*SNMP トラップの設定*『*148*p. 』」を参照してください。

設定したら、[Event Management - Destinations] (イベント管理 - 送信先) ページで SNMP トラップを有効にします。 「*[Event Management - Destinations] (イベント管理 - 送信先) の設定* 『*156*p. 』」を参照してください。

SNMP トラップの設定

Simple Network Management Protocol (SNMP) は、ネットワーク管理を制御し、ネットワーク デバイスとその機能を監視するためのプロトコルです。

SNMP トラップは、情報を収集するためにネットワーク上に送信されます。

SNMP トラップは、[Event Management - Settings] (イベント管理 - 設定) ページで設定されます。KX III SNMP トラップの一覧については、「KX III SNMP トラップのリスト」を参照してください。

SNMP に準拠したデバイスは、エージェントと呼ばれ、そのデバイスのデータを Management Information Bases (MIB) に格納し、SNMP トラップに応答します。

SNMP エージェントは、[Device Services] (デバイス サービス) ページで設定されます。SNMP エージェントの設定方法については、「*SNMP エージェントの設定* 『*145*p. 』」を参照し、KX III の MIB の表示方法については、「*KX III の MIB の表示* 『*154*p. 』」を参照してください。

▶ SNMP を設定する (SNMP のログ作成を有効にする) には、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Event Management - Settings] (イベント管理 - 設定) を選択します。[Event Management - Settings] (イベント管理 - 設定) ページが開きます。

2. [SNMP Logging Enabled] (SNMP ログを有効にする) チェックボックスをオンにすると、そのセクションの残りのチェックボックスが有効になります。**必ず入力してください。**
3. [SNMP v1/v2c Traps Enabled] (SNMP v1/v2c トラップを有効にする) または [SNMP Trap v3 Enabled] (SNMP Trap v3 トラップを有効にする) を選択するか、その両方を選択します。少なくとも 1 つのオプションを選択する必要があります。

   選択したら、関連するすべてのフィールドが有効になります。**必ず入力してください。**
4. SNMP v1/v2c 用の次のフィールドに入力します (必要な場合)。
   a. [Destination IP/Host Name] (送信先 IP/ホスト名) – SNMP マネージャの IP またはホスト名。最大 5 つの SNMP マネージャを作成できます。

   注: IPv6 アドレスでは、ホスト名が最大 80 文字です。

   ---
   b. [Port Number] (ポート番号) – SNMP マネージャで使用されるポート番号
   c. Community – デバイスのコミュニティ文字列

   注:SNMP コミュニティとは、SNMP を実行しているデバイスと管理ステーションが所属するグループのことです。SNMP コミュニティは、情報の送信先を定義するのに役立ちます。コミュニティ名は、グループを識別するために使用されます。SNMP デバイスや SNMP エージェントは、複数の SNMP コミュニティに所属できます。

   ---
5. [SNMP Trap v3 Enabled] (SNMP Trap v3 トラップを有効にする) チェックボックスをまだオンにしていない場合は、オンにすると、次のフィールドが有効になります。SNMP v3 用の次のフィールドに入力します (必要な場合)。
   a. [Destination IP/Host Name] (送信先 IP/ホスト名) – SNMP マネージャの IP またはホスト名。最大 5 つの SNMP マネージャを作成できます。

   注: IPv6 アドレスでは、ホスト名が最大 80 文字です。

   ---
   b. [Port Number] (ポート番号) – SNMP マネージャで使用されるポート番号
   c. [Security Name] (セキュリティ名) – SNMP エージェントと通信するエンティティのユーザ名またはサービス アカウント名 (32 文字以内)
   d. [Authentication Protocol] (認証プロトコル) – SNMP v3 エージェントで使用される MD5 または SHA 認証プロトコル
   e. [Authentication Passphrase] (認証パスフレーズ) – SNMP v3 エージェントへのアクセスに必要なパスフレーズ (64 文字以内)

f. [Privacy Protocol] (プライバシー プロトコル) – 必要に応じて PDU やコンテキスト データの暗号化に使用される AES または DES アルゴリズム

g. [Privacy Passphrase] (プライバシー パスフレーズ) – プライバシー プロトコル アルゴリズムへのアクセスに使用されるパスフレーズ (64 文字以内)

注:ローカル コンソールから [Event Management – Settings] (イベント管理 – 設定) ページにアクセスしており、画面解像度を 1280 x 1024 未満にしている場合、このページには [Privacy Passphrase] (プライバシー パスフレーズ) 列が表示されないことがあります。このような場合は、KX III の左パネルを非表示にします。「左パネル」を参照してください。

---

6. [OK] をクリックして、SNMP トラップを作成します。

[Link to SNMP Agent Configuration] (SNMP エージェント設定へのリンク) リンクを使用すると、[Event Management – Settings] (イベント管理 – 設定) ページから [Devices Services] (デバイス サービス) ページにすばやく移動できます。

SNMP トラップを設定するとキャプチャされるイベントは、[Event Management – Destinations] (イベント管理 – 送信先) ページで選択されます。「***[Event Management – Destinations] (イベント管理 – 送信先) の設定*** 『*156*p. 』」を参照してください。

KX III は、SNMP v1/v2c や v3 の SNMP ログをサポートします。SNMP ログが有効になっている場合は、SNMP v1/v2c で、メッセージ形式およびプロトコル操作が定義されます。SNMP v3 は SNMP のセキュリティを拡張したものであり、ユーザ認証、パスワード管理、および暗号化を提供します。

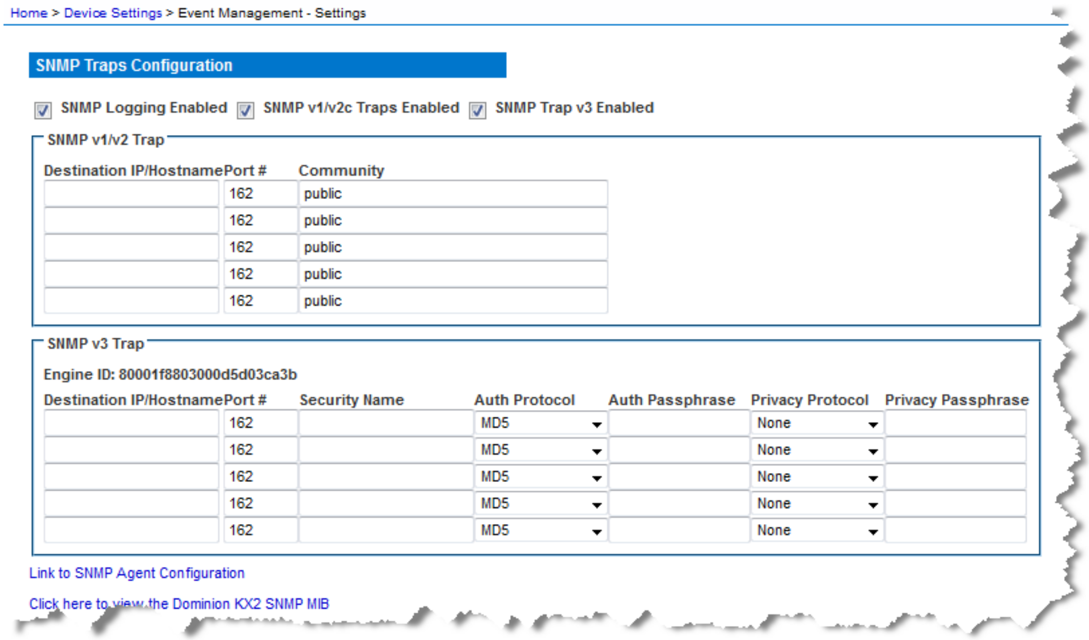
▶ 既存の SNMP トラップを編集するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Event Management – Settings] (イベント管理 – 設定) を選択します。[Event Management – Settings] (イベント管理 – 設定) ページが開きます。
2. 必要に応じて変更し、[OK] をクリックして変更を保存します。

注:どの時点で [SNMP Settings] (SNMP 設定) を無効にしても、SNMP 情報は保持されるので、設定を有効にし直す場合に再入力する必要はありません。

▶ SNMP トラップを削除するには、以下の手順に従います。

- SNMP トラップ フィールドをすべてクリアして保存します。



出荷時のデフォルトにリセットする機能を使用して、SNMP 設定を削除し、KX III を最初の出荷時のデフォルトに設定します。

▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

警告: UDP 経由の SNMP トラップを使用している場合は、KX III を再起動したときに KX III と接続先のルータが同期しなくなり、再起動完了の SNMP トラップがログ記録されなくなるおそれがあります。

KX III SNMP トラップのリスト

SNMP によって、トラップまたは通知を送信する機能と、1 つ以上の条件が満たされた場合に管理者に忠告する機能が提供されます。

KX III のトラップを次の表に示します。

トラップ名	説明
bladeChassisCommError	このポートに接続されているブレード シャーシ デバイスで通信エラーが検出されました。

トラップ名	説明
cimConnected	CIM は接続されています。
cimDisconnected	CIM は切断されています。
cimUpdateStarted	CIM の更新が開始されています。
cimUpdateCompleted	CIM の更新が完了しました。
configBackup	デバイス設定はバックアップされました。
configRestore	デバイス設定はリストアされました。
deviceUpdateFailed	デバイスの更新に失敗しました。
deviceUpgradeCompleted	RFP ファイルを使用した KX III のアップデートが完了しました。
deviceUpgradeStarted	RFP ファイルを使用した KX III のアップデートが開始されました。
factoryReset	デバイスが工場出荷時のデフォルトにリセットされました。
firmwareFileDiscarded	ファームウェア ファイルが破棄されました。
firmwareUpdateFailed	ファームウェアを更新できませんでした。
firmwareValidationFailed	ファームウェアの検証に失敗しました。
groupAdded	グループが KX III システムに追加されました。
groupDeleted	グループがシステムから削除されました。
groupModified	グループが変更されました。
ipConflictDetected	IP アドレスの競合が検出されました。
ipConflictResolved	IP アドレスの競合が解決されました。
networkFailure	製品の Ethernet インタフェースがネットワーク経由で通信できなくなりました。
networkParameterChanged	ネットワーク パラメータに変更が加えられました。
passwordSettingsChanged	強力なパスワードの設定が変更されました。
portConnect	以前認証されたユーザが KVM セッションを開始しました。
portConnectionDenied	ターゲット ポートへの接続が拒否されました。
portDisconnect	KVM セッションを実行中のユーザが正常にセッションを終了しました。

トラップ名	説明
portStatusChange	ポートが使用不可能な状態になっています。
powerNotification	電源コンセントの状態の通知です。1: アクティブ、0: 非アクティブ
powerOutletNotification	電源タップ デバイスのコンセントの状態の通知です。
rebootCompleted	KX III の再起動が完了しました。
rebootStarted	システムへの電源の入れ直しまたは OS からのウォーム起動により、KX III は再起動を開始しました。
scanStarted	ターゲット サーバのスキャンが開始されました。
scanStopped	ターゲット サーバのスキャンが停止されました。
securityBannerAction	セキュリティ バナーが承諾または拒否されました。
securityBannerChanged	セキュリティ バナーに変更が加えられました。
securityViolation	セキュリティ違反です。
setDateTime	デバイスの日付と時刻が設定されました。
setFIPSMode	FIPS モードが有効になりました。
startCCManagement	デバイスが CommandCenter の管理下におかれました。
stopCCManagement	デバイスが CommandCenter の管理下から除外されました。
userAdded	ユーザ アカウントがシステムに追加されました。
userAuthenticationFailure	不正なユーザ名または/およびパスワードでのログイン試行がありました。
userConnectionLost	あるユーザのアクティブ セッションが、タイムアウトにより異常終了しました。
userDeleted	ユーザ アカウントが削除されました。
userForcedLogout	ユーザは管理者によって強制的にログアウトされました。
userLogin	ユーザが KX III へ正常にログインし、認証され

トラップ名	説明
	ました。
userLogout	ユーザが KX III から正常にログアウトしました。
userModified	ユーザ アカウントが変更されました。
userPasswordChanged	デバイスのいずれかのユーザのパスワードが変更されると、このイベントが発生します。
userSessionTimeout	あるユーザのアクティブ セッションが、タイムアウトにより終了しました。
userUploadedCertificate	ユーザが SSL 証明書をアップロードしました。
vmImageConnected	ユーザが仮想メディアを使用してターゲットにデバイスまたはイメージのマウントを試みました。 デバイスまたはイメージのマッピング（マウント）が試行されるたびに、このイベントが生成されます。
vmImageDisconnected	ユーザが仮想メディアを使用してターゲットからデバイスまたはイメージのマウント解除を試みました。

KX III の MIB の表示

KX III の MIB を表示するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Event Management - Settings] (イベント管理 - 設定) を選択します。[Event Management - Settings] (イベント管理 - 設定) ページが開きます。
2. [Click here to view the Dominion KX3SNMP MIB] (Dominion KX3 SNMP MIB を表示するにはここをクリックします) リンクをクリックします。ブラウザ ウィンドウで MIB ファイルが開きます。

注:MIB ファイルに対して読み書き可能な場合は、MIB エディタを使用してファイルに変更を加えます。

```
-- This is a common MIB for Dominion KX/KSX G1 and KX/KSX G2 and LX traps

-- 12/20/11 H.
-- notifications updated
-- Added new traps for userDisconnectedFromPort

-- 07/08/11 H.
-- Corrected description for portStatusChange

-- 12/20/10 H.
-- notifications updated
-- Added new traps for scanStarted, scanStopped
-- Also added defn for portList

-- 03/09/10 H.
-- notifications updated
-- Added new traps for securityBannerChanged, securityBannerAction
-- Also added defn for bannerChanges, bannerAction

-- 09/08/09 H.
-- notifications updated
-- Added new traps for setDateTime, setFIPSMode
-- Also added defn for sysDateAndTime, fipsModeStatus

-- 10/14/08 H.
-- notifications updated
-- Added new traps for userForcedLogout, userUploadedCertificate
-- and bladeChassisCommError
-- Also added defn for certificateAuthorityName
```

syslog 設定

▶ **Syslog を設定する (Syslog の送信を有効にする) には、以下の手順に従います。**

1. [Enable Syslog Forwarding] (Syslog 送信有効) を選択して、リモート Syslog サーバにデバイス メッセージのログを送信します。
2. [IP Address] (IP アドレス) フィールドに Syslog サーバの IP アドレスまたはホスト名を入力します。
3. [OK] (OK) をクリックします。

注: IPv6 アドレスでは、ホスト名が最大 80 文字です。

デフォルトにリセットする機能を利用して、syslog 設定を削除します。

[Event Management - Destinations] (イベント管理 - 送信先) の設定

システム イベントを有効にすると、SNMP 通知イベント (トラップ) を生成できます。また、システム イベントを Syslog または監査ログにログ記録できます。[Event Management - Destinations] (イベント管理 - 送信先) ページを使用して、追跡するシステム イベントと、その情報の送信先を選択します。

注:SNMP トラップは、[SNMP Logging Enabled] (SNMP ログを有効にする) オプションが選択されている場合にのみ生成されます。一方、Syslog イベントは、[Enable Syslog Forwarding] (Syslog 送信有効) オプションが選択されている場合にのみ生成されます。これらのオプションは、いずれも [Event Management - Settings] (イベント管理 - 設定) ページで設定します。詳細については、「**[Event Management - Settings] (イベント管理 - 設定) の項目を設定する**」*(148p. の*「**[Event Management - Settings] (イベント管理 - 設定) の設定**」*参照)」を参照してください。*

▶ イベントとその送信先を選択するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Event Management - Destinations] (イベント管理 - 送信先) を選択します。[Event Management - Destinations] (イベント管理 - 送信先) ページが開きます。

   システム イベントは、デバイス操作、デバイス管理、セキュリティ、ユーザ アクティビティ、ユーザ グループ管理に分類されます。

2. 有効または無効にするイベント ラインのアイテムのチェックボックスと、情報の送信先のチェックボックスをオンにします。

   ヒント:[Category] (カテゴリ) チェックボックスをそれぞれオンまたはオフにすると、カテゴリ全体を有効または無効に設定できます。

   ---

3. [OK] をクリックします。

▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

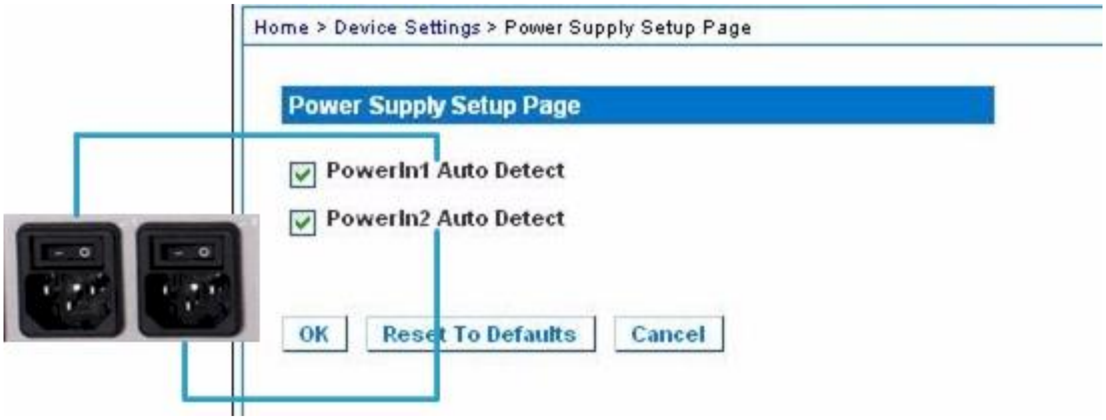
> 警告: UDP 経由の SNMP トラップを使用している場合は、KX III を再起動したときに KX III と接続先のルータが同期しなくなり、再起動完了の SNMP トラップがログ記録されなくなるおそれがあります。

[Power Supply Setup] (電源設定)

KX III にはデュアル電源が搭載されており、これらの電源の状態を検出し、通知できます。[Power Supply Setup] (電源設定) ページを使用して、片方の電源を使用しているのか、それとも両方の電源を使用しているのかを指定します。正しく設定することで、電源に障害が発生した場合に KX III によって適切な通知が送信されます。たとえば、1 番目の電源に障害が発生した場合は､ユニットの正面の電源 LED が赤色に変わります。

▶ 使用中の電源の自動検出を有効にするには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Power Supply Setup] (電源設定) を選択します。[Power Supply Setup] (電源設定) ページが開きます。



2. 電源入力を 1 番目の電源 (ユニット背面の左端の電源) に接続している場合は、[Powerln1 Auto Detect] (Powerln1 自動検出) チェックボックスをオンにします。
3. 電源入力を 2 番目の電源 (ユニット背面の右端の電源) に接続している場合は、[Powerln2 Auto Detect] (Powerln2 自動検出) チェックボックスをオンにします。
4. [OK] (OK) をクリックします。

注: これらのチェックボックスのいずれかをオンにしたにもかかわらず、電源入力が実際には接続されていない場合は、ユニット前面の電源 LED が赤色で点灯します。

自動検出を無効にするには、以下の手順に従います。

- 該当する電源のチェックボックスをオフにします。

工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

注: KX III では、CommandCenter に対して電源状態の報告を行いません。ただし、Dominion I (第 1 世代) では、CommandCenter に対して電源状態の報告を行います。

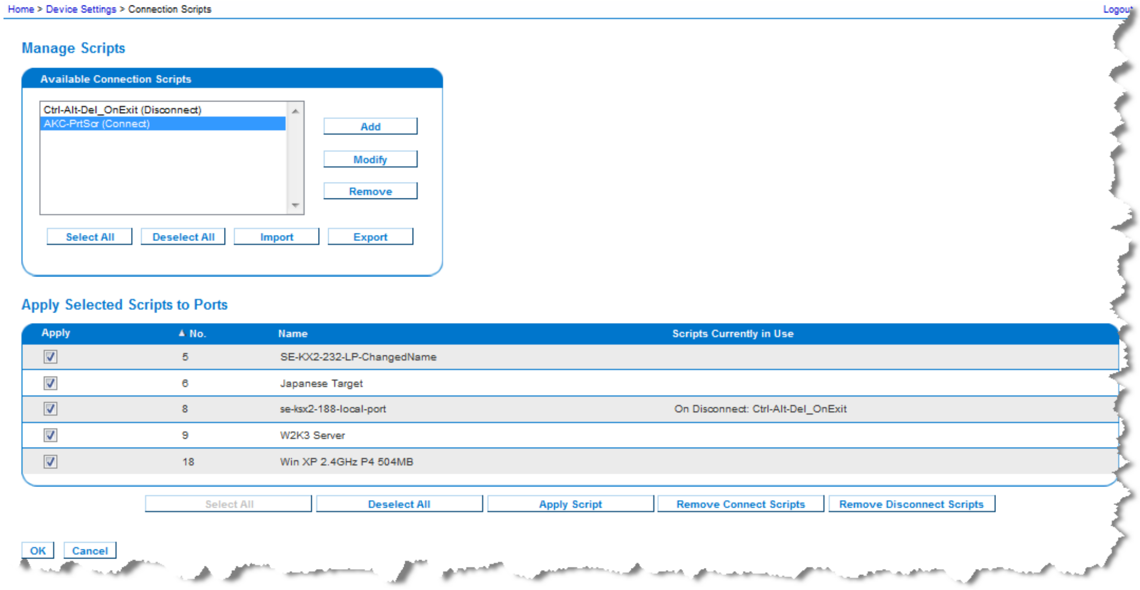
スクリプトの接続と切断

KX III では、ターゲットとの接続を確立または切断する場合にキー マクロ スクリプトを実行できます。

[Connection Scripts] (接続スクリプト) ページで独自のスクリプトを作成および編集し、ターゲットの接続を確立または切断するときに追加アクションを実行できます。

また、既存の XML ファイル形式の接続スクリプトをインポートすることもできます。KX III で作成したスクリプトを XML ファイル形式でエクスポートすることもできます。

KX III では、合計 16 個のスクリプトに対応できます。



スクリプトの適用および削除

▶ **スクリプトをターゲットに適用するには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、ターゲットに適用するスクリプトを選択します。'On Connect' スクリプトを 1 つと 'On Disconnect' スクリプトを 1 つターゲットに適用できます。

   注:ターゲットに一度に追加できるスクリプトは 1 つだけです。

   ---
3. [Apply Selected Scripts to Ports] (選択したスクリプトをポートに適用) セクションで、[Select All] (すべて選択) を使用するか、各ターゲットの左のチェックボックスをクリックして (選択したターゲットにのみスクリプトを適用する場合) スクリプトに適用するターゲットを選択します。
4. [Apply Scripts] (スクリプトを適用) をクリックします。スクリプトがターゲットに追加されると、それが [Apply Selected Scripts to Ports] (選択したスクリプトをポートに適用) セクションの [Scripts Currently in Use] (現在使用中のスクリプト] の下に表示されます。

▶ **スクリプトをターゲットから削除するには、以下の手順に従います。**

1. [Apply Selected Scripts to Ports] (選択したスクリプトをポートに適用) セクションで、[Select All] (すべて選択) を使用するか、各ターゲットの左のチェックボックスをクリックして (選択したターゲットからのみスクリプトを削除する場合) スクリプトを削除するターゲットを選択します。
2. [Remove Connect Scripts] (接続スクリプトを削除) をクリックして接続スクリプトを削除するか、[Remove Disconnect Scripts] (切断スクリプトを削除) をクリックして切断スクリプトを削除します。

スクリプトの追加

---
*注:KX III の外部で作成したスクリプトを追加したり、それらを XML ファイルとしてインポートしたりすることもできます。「***スクリプトのインポートとエクスポート***『162p. 』」を参照してください。*

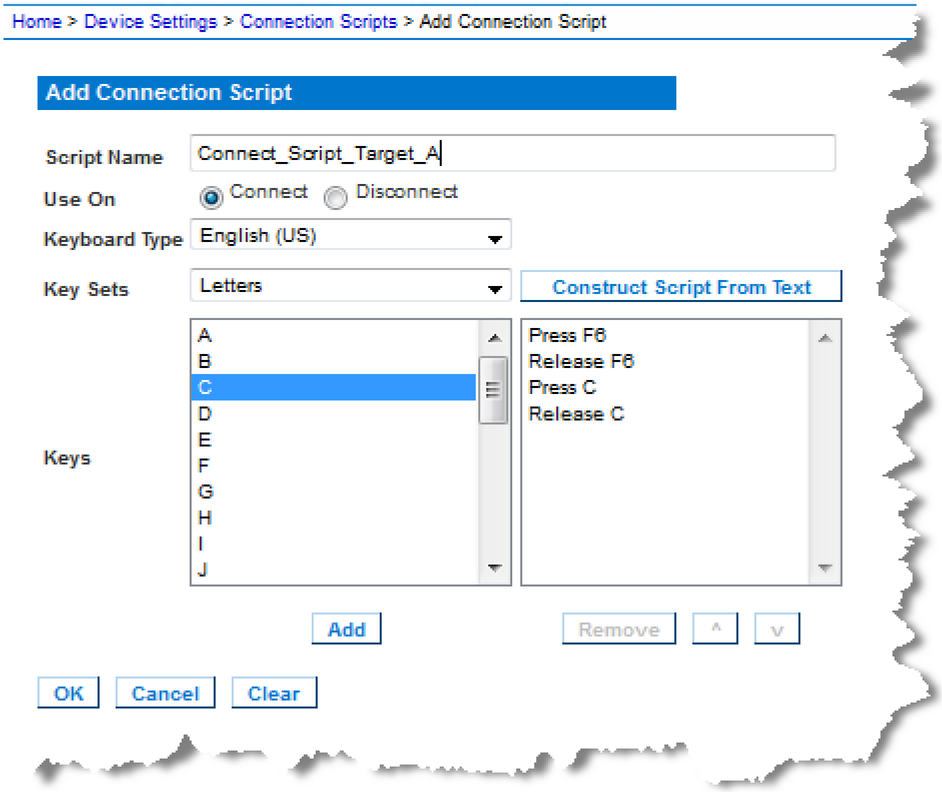
▶ **スクリプトを作成するには、以下の手順に従います。**

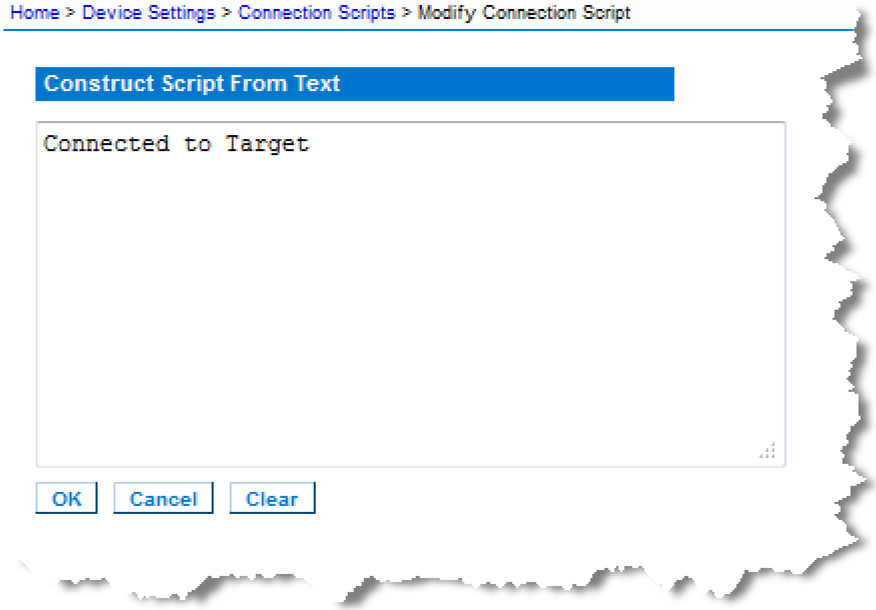
1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。

2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、[Add] (追加) をクリックします。[Add Connection Script] (接続スクリプトの追加) ページが開きます。
3. スクリプトの名前を最大 32 文字で入力します。スクリプトが作成されると、この名前が [Configure Scripts] (スクリプトの設定) ページの [Available Connection Scripts] (使用できる接続スクリプト) セクションに表示されます。
4. 作成中のスクリプトのタイプとして、[Connect] (接続) または [Disconnect] (切断) を選択します。接続スクリプトは、新規接続で、またはターゲットの切り替え時に使用されます。
5. 使用するターゲットで要求されるキーボード タイプを選択します。
6. [Key Sets] (キー セット) ドロップダウン リストから、スクリプトの作成に使用するキーボードのキー セットを選択します。選択すると、[Key Sets] (キー セット) ドロップダウン リストの下の [Add] (追加) ボックスに、選択したキー セット オプションが入力されます。
7. [Add] (追加) ボックスからキーを選択し、[Add] (追加) をクリックしてそれを [Script] (スクリプト) ボックスに移動します。キーを [Script] (スクリプト) ボックスから削除するには、キーを選択して [Remove] (削除) をクリックします。キーを並べ替えるには、それらを選択して [Up] (上へ) および [Down] (下へ) アイコンを使用します。

   スクリプトは、1 つ以上のキーで構成できます。また、スクリプトで使用されるキーを組み合わせることもできます。

   たとえば、F1 ～ F16 を選択すると、[Add] (追加) ボックスにファンクション キー セットが表示されます。ファンクション キーを選択して、それを [Script] (スクリプト) ボックスに移動します。次に、[Key Sets] (キー セット) ドロップダウン リストから [Letters] (文字) を選択して、文字キーをスクリプトに追加します。
8. スクリプトの実行時に表示されるテキストを追加することもできます。
   a. [Construct Script from Text] (テキストからスクリプトの作成) をクリックして、[Construct Script From Text] (テキストからスクリプトの作成) ページを開きます。
   b. テキスト ボックスにスクリプトを入力します。たとえば、「Connected to Target」(ターゲットに接続済み) と入力します。
   c. [Construct Script From Text] (テキストからスクリプトの作成) ページで [OK] をクリックします。
9. [OK] をクリックして、スクリプトを作成します。


Home > Device Settings > Connection Scripts > Add Connection Script
Add Connection Script
Script Name
Connect_Script_Target_A
Use On
Connect
Disconnect
Keyboard Type
English (US)
Key Sets
Letters
Construct Script From Text
Keys
A
B
C
D
E
F
G
H
I
J
Press F6
Release F6
Press C
Release C
Add
Remove
OK
Cancel
Clear


Home > Device Settings > Connection Scripts > Modify Connection Script
Construct Script From Text
Connected to Target
OK
Cancel
Clear

スクリプトの変更

▶ 既存のスクリプトを変更するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、変更するスクリプトを選択して、[Modify] (変更) をクリックします。ページが編集モードになります。
3. 必要に応じて変更します。完了したら [OK] をクリックします。

スクリプトのインポートとエクスポート

XML ファイル形式の接続スクリプトおよび切断スクリプトは、インポートおよびエクスポートできます。キーボード マクロのインポートまたはエクスポートはできません。

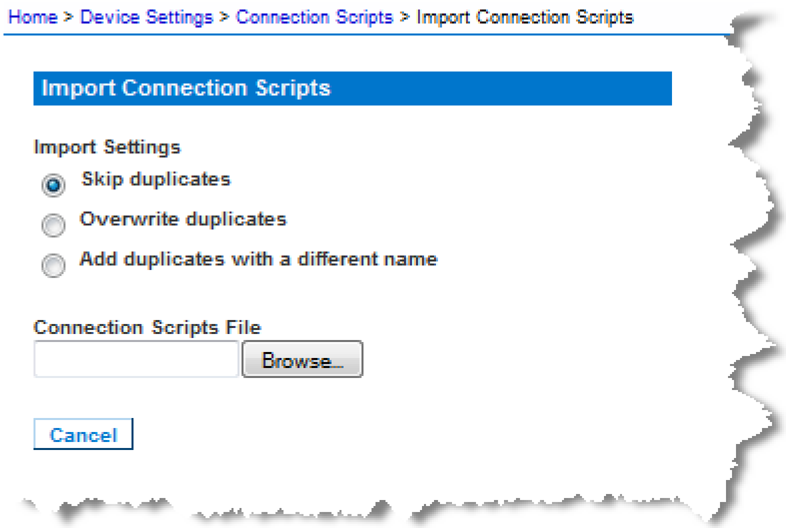
注:インポートおよびエクスポート機能は、ローカル コンソールからは使用できません。

インポートされたスクリプトは、KX III で変更機能を使用して編集できます。ただし、インポートされたスクリプトがポートに関連付けられると、変更できなくなります。変更するためには、ポートからスクリプトを削除します。「***スクリプトの適用および削除*** 『*159*p. 』」を参照してください。

▶ スクリプトをインポートするには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、[Import] (インポート) をクリックします。[Import Connection Scripts] (接続スクリプトのインポート) ページが開きます。
3. インポート設定を選択します。
   - [Skip duplicates] (重複をスキップ) – 既に KX III に存在するスクリプトは、インポートから除外されます。
   - [Overwrite duplicates] (重複を上書き) – 既に KX III に存在するスクリプトは、インポートされた新しいスクリプトで上書きされます。
   - [Add duplicates with a different name] (別の名前で重複を追加) – 重複スクリプトの名前がインポート中に変更されるので、既存のスクリプトは上書きされません。元のスクリプトと区別できるように、KX III によってファイル名に数字が割り当てられます。

4. 参照機能を使用して、インポートする XML スクリプト ファイルを検索します。
5. [Import] (インポート) をクリックします。[Configuration Scripts] (設定スクリプト) ページが開き、インポートされたスクリプトが表示されます。



▶ 切断スクリプトをエクスポートするには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Configuration Scripts] (設定スクリプト) をクリックします。[Configuration Scripts] (設定スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、エクスポートするスクリプトを選択して、[Export] (エクスポート) をクリックします。XML ファイルを開くか保存するためのダイアログ ボックスが表示されます。
3. XML ファイルを保存するか、XML エディタで開きます。XML ファイルを保存する場合は、デフォルトの Download フォルダに保存されます。

ポート グループ管理

ポート グループ管理では、以下が表示されます。

- [Blade Server Group] (ブレード サーバ グループ) – 特定のタイプのブレードに接続されるポートを、ブレード シャーシを示すグループにまとめたもの。詳細については、「*HP および Cisco UCS のブレード シャーシ設定 (ポート グループ管理)*『*117*p. 』」を参照してください。
- [Dual Video Port Group] (デュアル ビデオ ポート グループ) – ターゲット サーバ上で拡張デスクトップ設定を提供するポート グループの作成。「*デュアル ビデオ ポート グループの作成* 『*166*p. 』」を参照してください。
- [Port Group] (ポート グループ) – プライマリ ポートに適用されている設定がグループ内のすべてのセカンダリ ポートに適用される、「標準の」ポート グループの作成。「*ポート グループの作成*『*165*p. 』」を参照してください。

ポート グループの作成

KX III は、複数のポートをまとめた 1 つのポート グループをサポートします。ポート グループは、標準の KVM ポートとして設定されたポートだけで構成されます。ポートは、1 つのグループだけに属することができます。

ポート グループに追加可能なポートは、[Select Port for Group] (グループ化するポートの選択) の [Available] (利用可能) リストに表示されます。一度ポート グループに追加されたポートは、別のポート グループには追加できません。新しいポート グループでポートを使用するには、既存のポート グループからポートを削除します。

プライマリ ポートから実行される接続操作や切断操作は、電源制御を除いてグループ内のセカンダリ ポートに適用されます。

ポート グループは、[Backup and Restore] (バックアップとリストア) オプションを使用してリストアされます (「*バックアップと復元*『*192*p. 』」を参照してください)。

注:ブレード シャーシのポート グループを作成する方法については、「**HP および Cisco UCS のブレード シャーシ設定 (ポート グループ管理)**『117*p.* 』」*を参照し、デュアル ビデオ ポート グループを作成する方法については、「デュアル ビデオ ポート グループの作成」を参照してください。*

▶ ポート グループを作成するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Group Management] (ポート グループ管理) を選択します。[Port Group Management] (ポート グループ管理) ページが開きます。既存のポート グループすべてが表示されます。
2. [Add] (追加) をクリックします。ページが更新され、利用可能なポート グループ オプションがすべて表示されます。
3. [Port Group] (ポート グループ) ラジオ ボタンを選択します。
4. グループに追加するポートを選択するには、[Available] (利用可能) テキスト ボックス内のポートをクリックし、[Add] (追加) をクリックして該当するポートを [Selected] (選択) テキスト ボックスに追加します。
5. [OK] をクリックして、ポート グループを作成します。これで、[Port Group Management] (ポート グループ管理) ページにポート グループが表示されます。

デュアル ビデオ ポート グループの作成

デュアル ビデオ ポート グループ機能により、2 つのビデオ ポートを 1 つのグループにまとめることができます。この機能は、2 つのビデオ カードまたはビデオ ポートを搭載したサーバに接続する必要がある場合や、同じリモート クライアントから同時に両方のポートにアクセスする場合に使用します。

注:デュアル ポート ビデオ グループは、KX3-108 や KX3-116 のような、KVM チャネルが 1 つしかないモデルではサポートされていません。

注:デュアル ビデオ ポート グループは、作成すると、ローカル コンソールおよびリモート クライアントから利用できます。ただし、ローカル コンソールでは拡張デスクトップはサポートされていません。

デュアル ビデオ ポート グループは、[Port Access (ポート アクセス)] ページにデュアル ポート タイプとして表示されます。ポート グループに属しているプライマリ ポートおよびセカンダリ ポートは、[Port Access (ポート アクセス)] ページに、それぞれ [Dual Port(P) (デュアル ポート (P))] および [Dual Port(S) (デュアル ポート (S))] として表示されます。たとえば、CIM タイプが DCIM の場合は、[DCIM Dual Port (P) (DCIM デュアル ポート (P))] が表示されます。

各グループには、プライマリ ポートおよびセカンダリ ポートが含まれている必要があります。プライマリ ポートに適用される設定は、グループ内のすべてのセカンダリ ポートに適用されます。グループから削除されたポートは、独立したポートと見なされ、新しい設定を適用することができます。

リモート クライアントからデュアル ポート ビデオ グループにアクセスする場合は、プライマリ ポートに接続すると、デュアル ポート グループのプライマリ ポートとセカンダリ ポートの両方に対する KVM 接続ウィンドウが開きます。

セッションを開始し、必要に応じてリモート クライアントから 1 つ以上のモニタに表示できます。

デバイスで設定されている、ターゲットの方向設定が、ターゲットのオペレーティング システムでの実際の設定と一致している必要があります。

できる限り、接続元のクライアントの画面方向を同じに設定しておくことをお勧めします。

重要: 特定の環境に影響を与える可能性がある制限、推奨設定などについては、「デュアル ビデオ ポート グループ」の情報を確認してください。

デュアル ポート ビデオ グループを作成するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Group Management] (ポート グループ管理) を選択します。[Port Group Management] (ポート グループ管理) ページが開きます。既存のポート グループすべてが表示されます。
2. [Add] (追加) をクリックします。[Port Group] (ポート グループ) ページが開き、利用可能なすべてのポートが [Select Ports for Group] (グループ化するポートの選択) セクションに表示されます。

注:ポートが既にブレード サーバ ポート グループ、別のデュアル ビデオ ポート グループ、または「標準の」ポート グループに属している場合、そのポートを選択することはできません。これは、ポートは一度に 1 つのポート グループにしか属すことができないためです。

---

3. [Dual Video Port Group] (デュアル ビデオ ポート グループ) ラジオボタンを選択します。
4. [Select Ports for Group] (グループ化するポートの選択) セクションで、プライマリ ポートとして指定するポートをクリックし、[Add] (追加) をクリックして該当するポートを [Selected] (選択) テキスト ボックスに追加します。必ず最初にプライマリ ポートを追加してください。

---

*注: 理想的には、ポート グループの各ポートに適用される権限は同じでなければなりません。権限が同じでない場合は、最も制限の厳しいポートの権限がポート グループに適用されます。たとえば、あるポートに VM アクセスの拒否が適用されており、別のポートに VM アクセスの読み書きが適用されている場合、ポート グループには、VM アクセスの拒否が適用されます。ポートの権限がデュアル ビデオ ポート グループに与える影響については、**「***権限およびデュアル ビデオ ポート グループ アクセス***『227p. 』」を参照してください。*

---

5. セカンダリ ポートとして指定するポートをクリックし、[Add] (追加) をクリックして該当するポートを [Selected] (選択) テキスト ボックスに追加します。
6. ページの方向を選択します。選択する方向は、現在のモニタ設定に対する最適性によって異なります。
7. [OK] をクリックして、ポート グループを作成します。

   デュアル ビデオ ポート グループは、[Port Access (ポート アクセス)] ページにデュアル ポート タイプとして表示されます。ポート グループに属しているプライマリ ポートおよびセカンダリ ポートは、[Port Access (ポート アクセス)] ページに、それぞれ [Dual Port(P) (デュアル ポート (P))] および [Dual Port(S) (デュアル ポート (S))] として表示されます。たとえば、CIM タイプが DCIM の場合は、[DCIM Dual Port (P) (DCIM デュアル ポート (P))] が表示されます。

注:カスケード接続デバイスに接続されているデュアル ビデオ ポートのターゲットには、カスケード接続ベース デバイス以外のカスケード接続デバイスを介して接続する必要があります。

デフォルトの GUI 言語設定の変更

KX III の GUI は、デフォルトでは英語に設定されていますが、以下のローカライズ言語がサポートされています。

- 日本語
- [Simplified Chinese] (簡体字中国語)
- [Traditional Chinese] (繁体字中国語)

▶ GUI 言語を変更するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Language] (言語) を選択します。[Language Settings] (言語設定) ページが開きます。
2. [Language] (言語) ボックスの一覧で、GUI に適用する言語を選択します。
3. [Apply] (適用) をクリックします。[Reset Defaults] (デフォルトに戻す) をクリックして、[English] (英語) に戻します。

注:新しい言語を適用すると、オンライン ヘルプも、選択言語に合わせてローカライズされます。

セキュリティ上の問題

セキュリティの設定

[Security Settings] (セキュリティ設定) ページで、ログオン制限、ユーザ ブロック、パスワード ルール、および暗号化と共有に関する設定を行うことができます。

パブリック キーとプライベート キーの交換には Raritan SSL 証明書が使用され、セキュリティのレベルを高めます。Raritan の Web サーバ証明書は自己署名されています。Java アプレット証明書は、VeriSign の証明書によって署名されています。暗号化によって、情報が漏洩しないよう保護されていることが保証されます。また、これらの証明書によって、団体の身元が Raritan, Inc であることが立証されます。

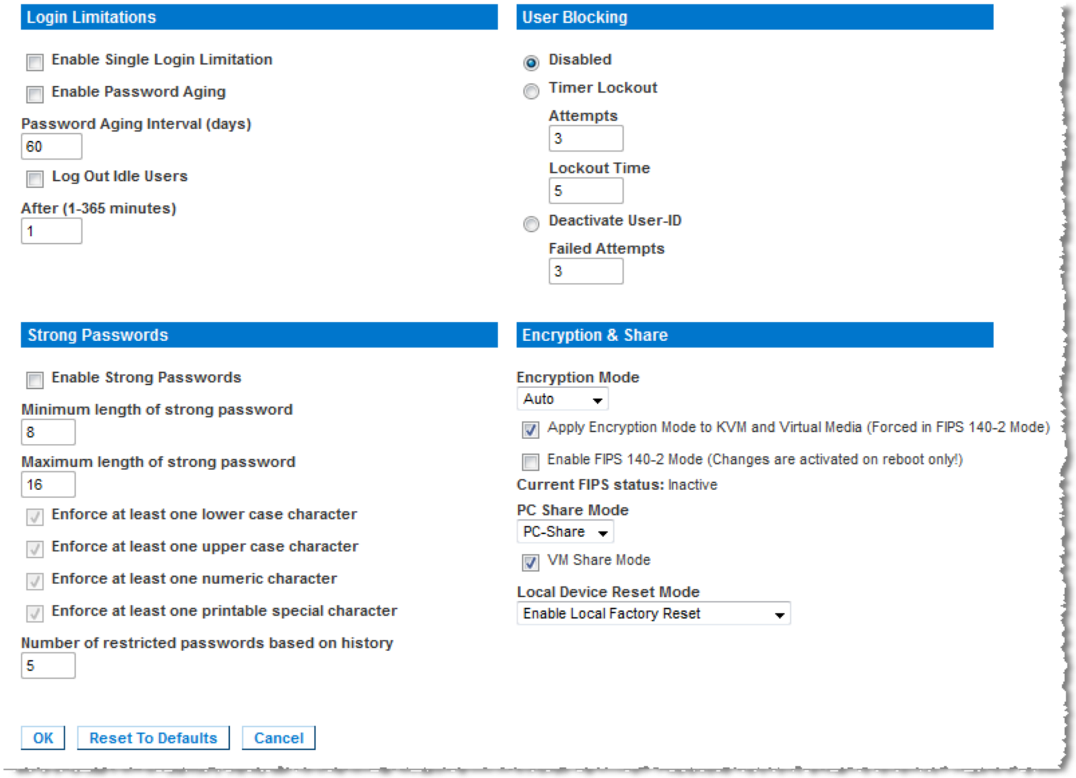
▶ セキュリティ設定を行うには、以下の手順に従います。

1. [Security] (セキュリティ) の [Security Settings] (セキュリティ設定) を選択します。[Security Settings] (セキュリティ設定) ページが開きます。
2. 必要に応じて、*[Login Limitations] (ログイン制限)* 『*169*p. 』 の設定を更新します。

3. 必要に応じて、*[Strong Passwords] (強力なパスワード)* 『*171*p. 』 の設定を更新します。
4. 必要に応じて、*[User Blocking] (ユーザ ブロック)* 『*173*p. の"*[ユーザ ブロック]*"参照 』 の設定を更新します。
5. 必要に応じて、[Encryption & Share] (暗号化および共有) の設定を更新します。
6. [OK] をクリックします。

▶ デフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

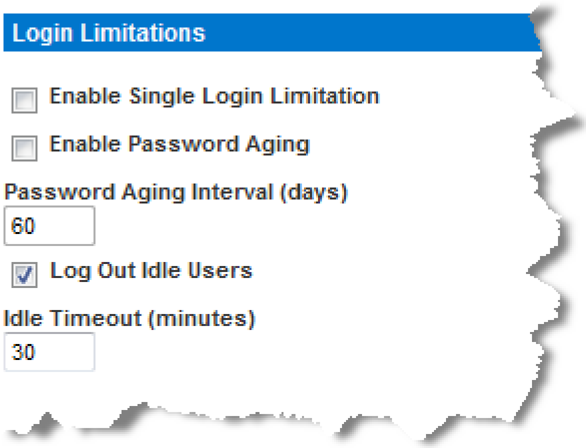


[Login Limitations] (ログイン制限)

ログイン制限を使用して、シングル ログイン、パスワード エージング、アイドル ユーザのログアウトに関する制限を指定できます。

制限	説明
[Enable Single Login Limitation] (シングル ログイン制限を	これを選択すると、常時ユーザ名ごとに 1 人のログインしか許可されません。このチェック ボックスをオフにした場合、所定のユーザ名とパス

制限	説明
有効にする)	ワードの組み合わせで、複数のクライアント ワークステーションからデバイスに同時接続できます。
[Enable password aging] (パスワード エージングを有効にする)	これを選択すると、[Password Aging Interval] (パスワード エージング間隔) フィールドで指定した日数に基づいて、すべてのユーザに対して定期的にパスワードを変更するよう要求します。 [Enable Password Aging] (パスワード エージングを有効にする) チェックボックスをオンにするとこのフィールドが有効になるため、設定する必要があります。パスワードの変更が要求される間隔を日数で入力します。デフォルトの日数は 60 日です。
[Log out idle users] (アイドル ユーザのログアウト)、[After (1-365 minutes)] (経過時間 (1 ～ 365 分))	[Log out idle users] (アイドル ユーザのログアウト) チェックボックスをオンにして、[After (1-365 minutes)] (経過時間 (1 ～ 365 分)) フィールドで指定した時間の経過後にユーザを自動的に切断します。キーボードまたはマウスで操作が行われない場合は、すべての セッションおよびすべてのリソースがログアウトされます。ただし、実行中の仮想メディア セッションはタイムアウトしません。 [After] (経過時間) フィールドは、アイドル ユーザがログアウトされるまでの時間 (分) を設定するために使用されます。このボックスが有効になるのは、[Log Out Idle Users] (アイドル ユーザをログオフする) チェック ボックスをオンにした場合です。フィールド値として最大 365 分を入力できます。



[Strong Passwords] (強力なパスワード)

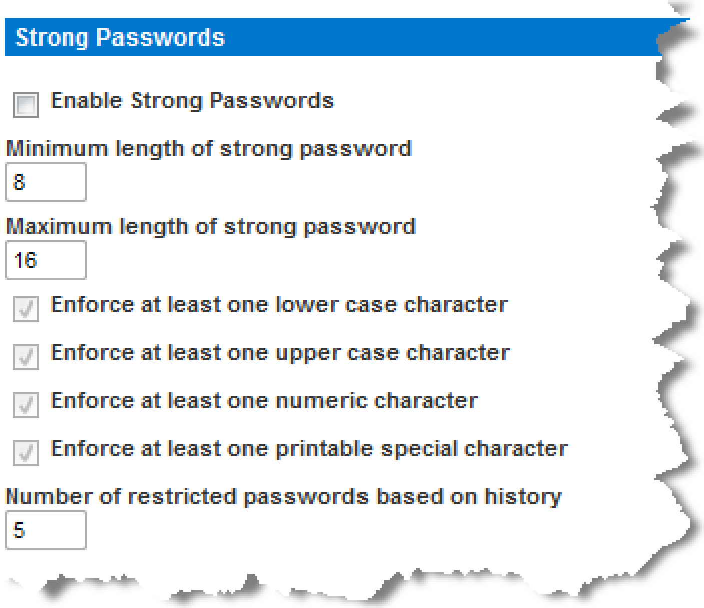
[Strong Passwords] (強力なパスワード) セクションで値を指定すると、このシステムにおけるローカル認証の安全性が高まります。強力なパスワードを使用すると、最小長と最大長、必要な文字、パスワード履歴の保持など、有効な KX III ローカル パスワードの形式を指定できます。

強力なパスワードには､アルファベットとアルファベット以外の文字 (句読点または数字) をそれぞれ 1 文字以上含むパスワードを指定する必要があります。また、パスワードとユーザ名の最初の 4 文字には同じ文字列を使用できません。

これを選択すると、強力なパスワードのルールが適用されます。パスワードが強力なパスワードの基準を満たしていない場合、ユーザは次回ログオンする際にパスワードを変更するよう自動的に求められます。[Enable Strong Passwords] (強力なパスワードを有効にする) チェック ボックスをオフにした場合、標準の形式になっているかどうかだけが検査されます。[Enable Strong Passwords] (強力なパスワードを有効にする) チェック ボックスをオンにした場合、次のフィールドが有効になるので、指定する必要があります。

フィールド	説明
[Minimum length of strong password] (強力なパスワードの最小長)	パスワードは 8 文字以上でなければなりません。デフォルトでは 8 文字ですが、管理者は最小長を 63 文字に変更することができます。
[Maximum length of strong password] (強力なパスワードの最大長)	デフォルトの最小長は 8 文字ですが、管理者は最大長をデフォルトの 16 文字に設定することができます。強力なパスワードの最大長は 63 文字です。
[Enforce at least one lower	これを選択すると、パスワードに 1 文

フィールド	説明
case character] (1 文字以上の小文字の使用を強制する)	字以上の小文字が必要になります。
[Enforce at least one upper case character] (1 文字以上の大文字の使用を強制する)	これを選択すると、パスワードに 1 文字以上の大文字が必要になります。
[Enforce at least one numeric character] (1 文字以上の数字の使用を強制する)	これを選択すると、パスワードに 1 文字以上の数字が必要になります。
[Enforce at least one printable special character] (1 文字以上の印刷可能な特殊文字の使用を強制する)	これを選択すると、パスワードに 1 文字以上の印刷可能な特殊文字が必要になります。
[Number of restricted passwords based on history] (履歴に基づく制限パスワードの数)	このフィールドは、パスワード履歴数を表します。つまり、繰り返し使用できない以前のパスワードの数を表します。範囲は 1 ～ 12 で、デフォルトは 5 です。



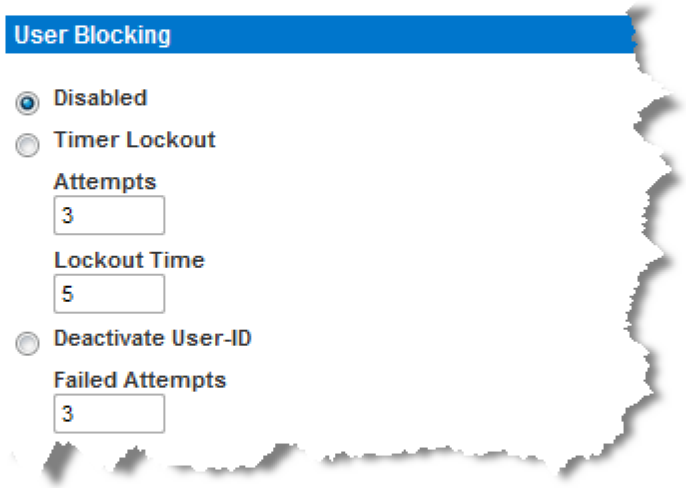
[ユーザ ブロック]

[ユーザ ブロック] セクションでは基準を指定し、ユーザが指定回数ログオンに失敗するとシステムにアクセスできなくなるようにします。

次の 3 つのオプションは、相互に排他的です。

オプション	説明
[無効]	デフォルト値です。認証に失敗した回数に関わらず、ユーザのアクセスはブロックされません。

オプション	説明
[タイマ ロックアウト]	ユーザが指定回数より多くログオンに失敗すると、システムへのアクセスが指定の時間拒否されます。これを選択した場合は次のフィールドが有効になります。 ▪ [試行回数]: この回数より多くログオンに失敗すると、ユーザはロックアウトされます。有効な範囲は 1 ～ 10 で、デフォルトの試行回数は 3 です。 ▪ [ロックアウト時間]: ユーザがロックアウトされる時間です。有効な範囲は 1 ～ 1440 分で、デフォルトでは 5 分です。 *注: [タイマ ロックアウト] で指定した値は、Administrator の役割が割り当てられているユーザには適用されません。*
[ユーザ ID を無効化]	このオプションを選択した場合は、[試行回数] フィールドで指定した回数より多くログオンに失敗すると、ユーザはシステムからロックアウトされます。 ▪ [試行回数]: この回数より多くログオンに失敗すると、そのユーザのユーザ ID が無効になります。このボックスが有効になるのは、[ユーザ ID を無効化] オプションを選択した場合です。有効な範囲は 1 ～ 10 です。 指定回数より多くログオンに失敗してユーザ ID が無効になった場合、管理者はユーザ パスワードを変更し、[ユーザ] ページの [有効化] チェックボックスをオンにしてユーザ アカウントを有効化する必要があります。



[Encryption & Share] (暗号化および共有)

[Encryption & Share] (暗号化および共有) セクションでは、使用する暗号化のタイプ、PC と VM の共有モード、KX III のリセット ボタンを押したときに実行されるリセットのタイプを指定できます。

> 警告: ご使用のブラウザでサポートされていない暗号化モードを選択した場合、そのブラウザから KX III にアクセスできなくなります。

暗号化および共有の設定

暗号化が適用されると、ビデオ パフォーマンスが低下する場合があります。パフォーマンス低下の程度は、暗号化モードによって異なります。

ビデオ パフォーマンスおよびスループットを最高にする場合は、暗号化を無効にします。ただし、セキュリティ ポリシーで許されている場合に限ります。

▶ 暗号化および共有を設定するには、以下の手順に従います。

1. [Encryption Mode] (暗号化モード) ボックスの一覧で暗号化モードを選択します。

   選択した暗号化モードがご使用のブラウザでサポートされていない場合 KX III に接続できない、という内容の警告が表示されます。

   この警告は、"暗号化モードを選択する際、ご使用のブラウザでその暗号化モードがサポートされていることを確認してください。サポートされていない場合、KX III に接続できません" という意味です。

暗号化モード	説明
自動	これは推奨オプションです。使用可能な最高強度の暗号化モードに自動設定されます。

暗号化モード	説明
	デバイスとクライアントが FIPS 準拠アルゴリズムの使用を正常にネゴシエートできるようにするには、[Auot] (自動) を選択する必要があります。
[RC4] (RC4)	RSA RC4 暗号方式を使用して、ユーザ名、パスワード、ビデオ送信を含む KVM データが保護されます。これは、最初の接続認証中に KX III とリモート PC 間のプライベート通信チャンネルを提供する 128 ビットの SSL (セキュア ソケット レイヤ) プロトコルです。 FIPS 140-2 モードを有効にして [RC4] (RC4) を選択すると、エラー メッセージが表示されます。[RC4] (RC4) は FIPS 140-2 モードでは使用できません。
[AES-128]	AES (Advanced Encryption Standard) は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。"128" はキーの長さを意味します。[AES-128] (AES-256) を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。詳細については、「***ご使用のブラウザで AES 暗号化モードがサポートされているかどうかを確認する*** 『***178***p. の"***ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する***"参照 』」を参照してください。
[AES-256]	AES (Advanced Encryption Standard) は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。"256" はキーの長さを意味します。[AES-256] (AES-256) を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。詳細については、「***ご使用のブラウザで AES 暗号化モードがサポートされているかどうかを確認する*** 『***178***p. の"***ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する***"参照 』」を参照してください。

注: Windows XP® (Service Pack 2 適用) と Internet Explorer® 7 を使用している場合、AES-128 暗号化モードで KX III にリモート接続することはできません。

2. [Apply Encryption Mode to KVM and Virtual Media] (暗号化モードを KVM および仮想メディアに適用する) チェック ボックスの値を指定します。このチェック ボックスをオンにした場合、選択した暗号化モードが KVM と仮想メディアの両方に適用されます。認証後、KVM データと仮想メディア データが 128 ビットの暗号化モードで転送されます。
3. 政府やその他のセキュリティの高い環境では、[Enable FIPS 140-2] (FIPS 140-2 を有効にする) チェックボックスをオンにして FIPS 140-2 モードを有効にします。FIPS 140-2 を有効にする方法については、「***FIPS 140-2 の有効化*** 『*179*p. 』」を参照してください。
4. [PC Share Mode] (PC 共有モード) - グローバルな同時リモート KVM アクセスを特定し、最大 8 人までのリモート ユーザが KX III に同時にログオンし、デバイスを介してターゲット サーバを同時に表示および制御できるようにします。次のいずれかのオプションを選択します。
   - [Private] (プライベート): PC を共有しません。これはデフォルト値です。一度に 1 人のユーザが、排他的に各ターゲット サーバにアクセスできます。
   - [PC-Share] (PC 共有): KVM ターゲット サーバに最大 8 人のユーザ (管理者または非管理者) が同時にアクセスできます。ただし、リモート ユーザはキーボートやマウスで全く同じ操作を行えるため、文字の入力やマウスの操作を止めないユーザがいると、制御が不規則になる場合があることに注意してください。
5. 必要に応じて、[VM Share Mode] (VM 共有モード) チェック ボックスをオンにします。このチェック ボックスは [PC-Share Mode] (PC 共有モード) ボックスの一覧で [PC-Share] (PC 共有) を選択した場合にのみ有効になります。このオプションを選択すると、複数のユーザで仮想メディアを共有できるようになります。つまり、複数のユーザが同じ仮想メディア セッションにアクセスできます。デフォルトでは、このチェック ボックスはオフになっています。
6. 必要に応じて、[Local Device Reset Mode] (ローカル デバイス リセット モード) ボックスの一覧で値を選択します。このオプションでは、ユニットの背面にあるハードウェア リセット ボタンが押下された際に実行するアクションを指定します。詳細については、「リセット ボタンを使用して KX III をリセットする」を参照してください。次のいずれかの値を選択します。

ローカル デバイス リセット モード	**説明**
[Enable Local Factory	KX III を出荷時設定にリセットします。

ローカル デバイス リセット モード	説明
Reset] (ローカルで出荷時設定にリセットする) (デフォルト)	
[Enable Local Admin Password Reset] (ローカルで管理者パスワードだけをリセットする)	ローカルの管理者パスワードだけをリセットします。パスワードは raritan に戻ります。
[Disable All Local Resets] (ローカルでリセットしない)	リセットは一切実行されません。

注:P2CIM-AUSBDUAL または P2CIM-APS2DUAL を使用してターゲットを 2 台の KX III に接続しており、かつ、ターゲットへのプライベート アクセスが必要である場合、両方の KX III において PC 共有モードを [Private] (プライベート) に設定する必要があります。

Paragon CIM と ProductName を組み合わせて使用する場合の詳細については、「サポートされている Paragon CIM および設定 『317*p.* の"サポートされている Paragon II CIMS および設定"参照 』」*を参照してください。*

ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する

ブラウザで AES が使用されているかどうかわからない場合は、ブラウザの製造元に問い合わせるか、暗号化方法を調べたいブラウザを使用して https://www.fortify.net/sslcheck.html Web サイトにアクセスしてください。この Web サイトでは、ブラウザの暗号化方法が検出され、レポートが表示されます。

AES 256 ビット暗号化方式は、以下のブラウザでサポートされています。

- Firefox®
- Internet Explorer®

AES 256 ビット暗号化方式を使用するには、サポート対象ブラウザを使用することに加え、Java™ Cryptography Extension® (JCE®) 無制限強度の管轄ポリシー ファイルをインストールする必要があります。

各種 JRE™ の管轄ファイルは、次のページの [other downloads] セクションで入手できます。

- JRE1.7 - javase/downloads/jce-7-download-432124.html

FIPS 140-2 の有効化

政府やその他のセキュリティの高い環境では、場合によっては、FIPS 140-2 モードを有効にする必要があります。

KX III では、『FIPS 140-2 Implementation Guidance』(FIPS 140-2 実装ガイダンス) の G.5 セクションのガイドラインに従って、Linux® プラットフォームで実行されている FIPS 140-2 で検証された埋め込み暗号化モジュールが使用されます。

このモードを有効にすると、SSL 証明書の生成に使用される秘密鍵を内部で生成する必要があり、ダウンロードしたりエクスポートしたりすることはできません。

FIPS 140-2 モードを有効にすると、パフォーマンスが低下する場合があります。

FIPS 140-2 を有効にするには、以下の手順に従います。

1. [Security Settings] (セキュリティ設定) ページを開きます。
2. [Security Settings] (セキュリティ設定) ページの [Encryption & Share] (暗号化および共有) セクションで [Enable FIPS 140-2] (FIPS 140-2 を有効にする) チェックボックスをオンにして、FIPS 140-2 モードを有効にします。

   FIPS 140-2 モードでは、外部通信に FIPS 140-2 で承認されたアルゴリズムを利用します。

   ビデオ、キーボード、マウス、仮想メディア、およびスマート カードのデータで構成される KVM セッション トラフィックの暗号化には、FIPS 暗号化モジュールが使用されます。
3. KX III を再起動します。**必ず入力してください。**

   FIPS モードが有効になると、「FIPS Mode: Enabled」(FIPS モード: 有効) というメッセージが画面の左パネルの [Device Information] (デバイス情報) セクションに表示されます。

   FIPS モードが有効になったら、セキュリティを強化するために、新しい証明書署名要求を作成することもできます。この要求は、必要な鍵暗号を使用して作成されます。署名された証明書をアップロードするか、自己署名証明書を作成します。SSL 証明書の状態は、[Not FIPS Mode Compliant] (FIPS モード非準拠) から [FIPS Mode Compliant] (FIPS モード準拠) に更新されます。

   FIPS モードが有効になっている場合は、鍵ファイルをダウンロードまたはアップロードできません。最後に作成された CSR が内部で鍵ファイルに関連付けられます。さらに、CA からの SSL 証明書とその秘密鍵は、バックアップされたファイルの完全な復元に含まれません。鍵を KX III からエクスポートすることはできません。

FIPS 140-2 サポートの要件

KX III では、FIPS 140-2 で承認された暗号化アルゴリズムの使用がサポートされます。これにより、クライアントが FIPS 140-2 専用モードに設定されている場合に、SSL サーバとクライアントでは、暗号化されたセッションに使用されている暗号スイートを正常にネゴシエートできます。

KX III で FIPS 140-2 を使用する場合の推奨事項を以下に示します。

KX III

- [Security Settings] (セキュリティ設定) ページで、[Encryption & Share] (暗号化および共有) を [Auto] (自動) に設定します。「暗号化および共有」を参照してください。

Microsoft クライアント

- クライアント コンピュータと Internet Explorer で FIPS 140-2 を有効にする必要があります。

▶ Windows クライアントで FIPS 140-2 を有効にするには、以下の手順に従います。

1. [コントロール パネル]、[管理ツール]、[ローカル セキュリティ ポリシー] の順に選択して、[ローカル セキュリティ設定] ダイアログ ボックスを開きます。
2. ナビゲーション ツリーで、[ローカル ポリシー]、[セキュリティ オプション] の順に選択します。
3. [システム暗号化: 暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う] を有効にします。
4. クライアント コンピュータを再起動します。

▶ Internet Explorer で FIPS 140-2 を有効にするには、以下の手順に従います。

1. Internet Explorer で、[ツール] の [インターネット オプション] を選択し、[詳細設定] タブをクリックします。
2. [TLS 1.0 を使用する] チェックボックスをオンにします。
3. ブラウザを再起動します。

IP アクセス制御を設定する

IP アクセス制御機能を利用することにより、KX III に対するアクセスを制御できます。IP アクセス制御では、あらゆるタイプのトラフィックによる KX III へのアクセスが制限されるので、NTP サーバ、RADIUS ホスト、DNS ホストなどは、KX III へのアクセスが許可されている必要があります。

グローバル アクセス制御リスト（ACL）の設定を行い、許可されていない IP アドレスから送信されるパケットにデバイスが応答することのないようにします。IP アクセス制御はグローバルに作用し、KX III 全体に影響しますが、グループ レベルで KX III へのアクセスを制御することもできます。グループ レベルの制御の詳細については、「*グループ ベースの IP アクセス制御リスト*『*63*p. の"*グループベースの IP ACL（アクセス制御リスト）*"参照 』」を参照してください。

重要: KX III のローカル ポートでは、IP アドレス 127.0.0.1 が使用されます。IP アクセス制御リストを作成する際に、ブロックされる IP アドレス範囲に 127.0.0.1 を含めないでください。そうしなければ、KX III ローカル ポートにアクセスできなくなります。

▶ IP アクセス制御機能を利用するには

1. [Security]（セキュリティ）の [IP Access Control]（IP アクセス制御）を選択すると、[IP Access Control]（IP アクセス制御）ページが開きます。
2. [Enable IP Access Control]（IP アクセス制御を有効にする）チェック ボックスをオンにし、このページの他のフィールドを有効にします。
3. [Default policy]（デフォルト ポリシー）ボックスの一覧で値を選択します。これは、指定した範囲内にない IP アドレスに対して実行されるアクションです。
   - [ACCEPT]（許可）: 指定した範囲内にない IP アドレスから KX III へのアクセスを許可します。
   - [Drop]（拒否）: 指定した範囲内にない IP アドレスから KX III へのアクセスを拒否します。

▶ ルールを一覧の末尾に追加するには

1. [IPv4/Mask or IPv6/Prefix Length]（IPv4/マスクまたは IPv6/プレフィックスの長さ）ボックスに IP アドレスとサブネット マスクを入力します。

   注: IP アドレスは Classless Inter-Domain Routing (CIDR) 方式で入力してください。つまり、先頭の 24 ビットをネットワーク アドレスとして使用します。

2. [Policy]（ポリシー）列のボックスの一覧でポリシーを選択します。

3. [Append] (追加) をクリックします。そのルールがルール一覧の末尾に追加されます。

▶ ルールを一覧の途中に挿入するには

1. ルール番号を入力します。ルールを一覧の途中に挿入する場合、ルール番号は入力必須です。
2. [IPv4/Mask or IPv6/Prefix Length] (IPv4/マスクまたは IPv6/プレフィックスの長さ) ボックスに IP アドレスとサブネット マスクを入力します。
3. [Policy] (ポリシー) 列のボックスの一覧でポリシーを選択します。
4. [Insert] (挿入) をクリックします。入力したルール番号と同じルール番号のルールが存在する場合、新しいルールはそのルールの上に挿入され、以降のすべてのルールが 1 行下に下がります。

> ヒント: ルール番号を使用すると、各ルールを作成する順序を気にせずに済みます。

▶ ルールの内容を置換するには

1. 置換したいルールのルール番号を入力します。
2. [IPv4/Mask or IPv6/Prefix Length] (IPv4/マスクまたは IPv6/プレフィックスの長さ) ボックスに IP アドレスとサブネット マスクを入力します。
3. [Policy] (ポリシー) 列のボックスの一覧でポリシーを選択します。
4. [Replace] (置換) をクリックします。同じルール番号の既存ルールが、新しいルールに置き換わります。

▶ ルールを削除するには

1. 削除したいルールのルール番号を入力します。
2. [Delete] (削除) をクリックします。

3. 削除してよいかどうかを確認するダイアログ ボックスが開きます。[OK] (OK) をクリックします。

SSL 証明書

KX III では、接続先クライアントとの間で送受信されるトラフィックを暗号化するために Secure Sockets Layer (SSL) が使用されます。

KX III とクライアントとの接続を確立する際、暗号化された証明書を使用して、KX III の正当性をクライアントに示す必要があります。

KX III 上で、証明書署名要求 (CSR) を生成し、証明機関 (CA) によって署名された証明書をインストールすることができます。

CA はまず、CSR 発行元の身元情報を検証します。

続いて、署名された証明書を発行元に返します。有名な CA によって署名されたこの証明書は、証明書発行者の身元を保証する目的で使用されます。

重要: KX III の日付と時刻が正しく設定されていることを確認します。

自己署名証明書が作成されると、KX III の日付と時刻を使用して、有効期間が計算されます。KX III の日付と時刻が正確でない場合、証明書の有効な日付範囲が正しくなくなり、証明書の検証に失敗するおそれがあります。「*日付/時刻の設定* 『*147*p. 』」を参照してください。

注:CSR は、KX III で生成する必要があります。

注: ファームウェアをアップグレードしても、アクティブな証明書および CSR は置き換えられません。

SSL 証明書を作成してインストールするには

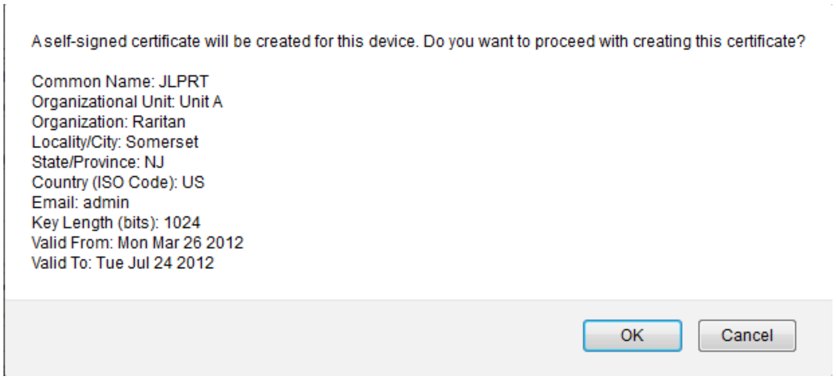
1. [Security] (セキュリティ) メニューの [Certificate] (証明書) を選択します。
2. 次の各フィールドの値を指定します。
   a. [Common name] (共通名) – KX III をネットワークに追加したときに指定した、KX III のネットワーク名。通常は完全修飾ドメイン名です。共通名は、Web ブラウザで KX III にアクセスする際に使用する名前から、プレフィックスである「http://」を除いたものです。ここで指定した名前が実際のネットワーク名と異なる場合は、HTTPS を使用して KX III にアクセスする際に、ブラウザでセキュリティ警告が表示されます。
   b. [Organizational unit] (組織内部門): KX III が属する、組織内の部門。
   c. [Organization] (組織): KX III が属する組織。
   d. [Locality/City] (市区町村): 組織が存在する市区町村。
   e. [State/Province] (都道府県): 組織が存在する都道府県。
   f. [Country (ISO code)] (国 (ISO コード)): 組織が存在する国。2 文字の ISO コードを入力します。たとえば、ドイツの場合は「DE」、米国の場合は「US」と入力します。
   g. [Challenge Password] (チャレンジ パスワード): 一部の CA は、証明書が失効した場合などに証明書の変更を許可するための、チャレンジ パスワードを要求します。CA 証明書の CSR を生成するときに適用されます。
   h. [Confirm Challenge Password] (チャレンジ パスワードの確認入力): 確認のためチャレンジ パスワードを再度入力します。CA 証明書の CSR を生成するときに適用されます。
   i. [Email] (電子メール): KX III とそのセキュリティを担当する人の電子メール アドレス。
   j. [Key length (bits)] (キー長 (単位: ビット)): 生成されるキーの長さ (単位: ビット)。デフォルト値は [1024] (1024) です。
3. 生成するには、次のいずれかの手順に従います。
   - 自己署名証明書を生成するには、以下の手順に従います。

a. 自己署名証明書を生成する必要がある場合は、[Create a Self-Signed Certificate] (自己署名証明書の作成) チェックボックスをオンにします。このオプションを選択すると、入力内容に基づいて証明書が生成され、KX III が署名証明機関として機能します。CSR をエクスポートして署名入り証明書の生成に使用する必要はありません。

b. 有効期限の日数を指定します。KX III の日付と時刻が正しいことを確認し、正しくない場合は、有効な日付を使用して、証明書の有効期限を作成できます。

c. [Create] (作成) をクリックします。

d. 確認ダイアログ ボックスが表示されます。[OK] をクリックして、ダイアログ ボックスを閉じます。

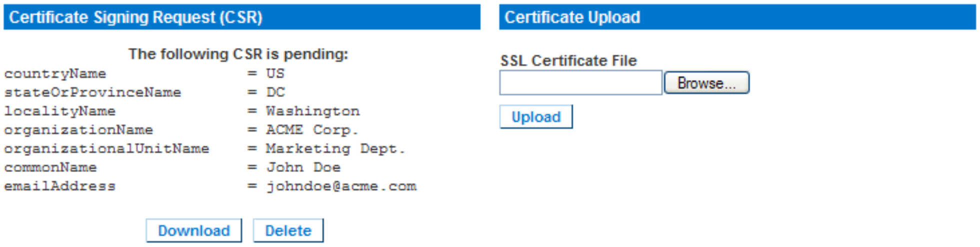


e. KX III を再起動して自己署名証明書を有効にします。

- CSR を生成して証明書の CA に送信するには、以下の手順に従います。

a. [Create] (作成) をクリックします。

b. 入力したすべての情報を含むメッセージが表示されます。



c. CSR、および CSR 生成時に使用された秘密鍵を含むファイルをダウンロードするには、[Download CSR] (CSR のダウンロード) をクリックします。

d. 証明書を取得するため、保存されている CSR を CA に送信します。CA から新しい証明書が届きます。

注: CSR と秘密鍵ファイルはセットになっているので、そのように扱う必要があります。署名付き証明書が、元の CSR の生成時に使用された秘密鍵と対応していない場合、その証明書は使用できません。このことは、CSR と秘密鍵ファイルのアップロードおよびダウンロードに当てはまります。

- CA から証明書を取得したら、[Upload] (アップロード) をクリックして KX III にアップロードします。
- KX III を再起動して証明書を有効にします。

この手順が完了すると、KX III 専用の証明書が入手されます。この証明書は、KX III の身元をクライアントに対して示す際に使用されます。

重要: KX III 上の CSR を破棄した場合、復旧する方法はありません。誤って CSR を削除してしまった場合、前述の 3 つの手順をやり直す必要があります。やり直しを回避するには、ダウンロード機能を利用し、CSR とその秘密鍵のコピーを取得しておきます。

セキュリティ バナー

KX III ログイン プロセスにセキュリティ バナーを追加できます。この機能により、ユーザは、KX III にアクセスできるようになる前に、セキュリティ同意書に同意するかどうかの選択を求められます。セキュリティ バナーの内容は、ユーザが自分のログイン資格情報を使用して KX III にアクセスした後、[Restricted Service Agreement] (制限付きサービス同意書) ダイアログ ボックスに表示されます。

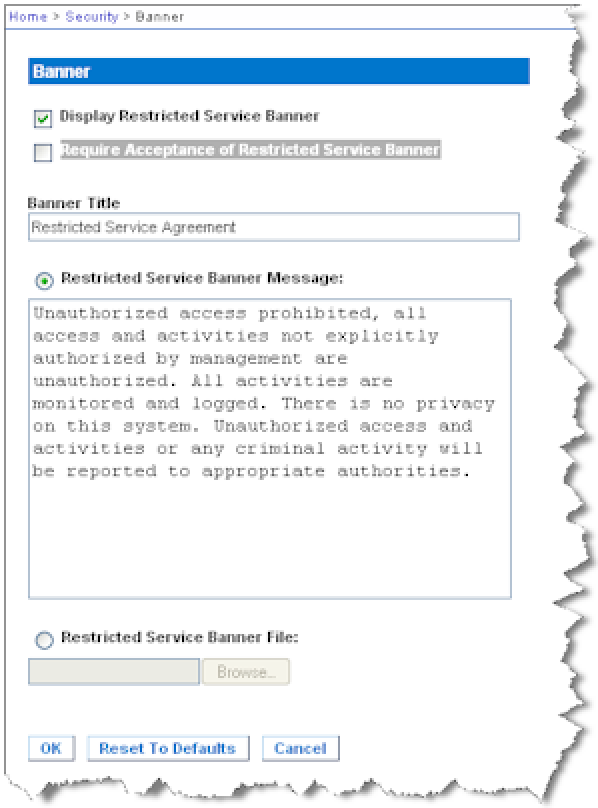
セキュリティ バナーの見出しおよび本文はカスタマイズできます。デフォルトのテキストをそのまま使用することもできます。また、セキュリティ バナーは、ユーザがセキュリティ同意書に同意してからでないと KX III にアクセスできないように設定することも、単にログイン プロセス終了後に表示することもできます。同意/不同意機能が有効になっている場合、ユーザが選択した内容が監査ログに記録されます。

▶ セキュリティ バナーを設定するには

1. [Security] (セキュリティ) − [Banner] (バナー) をクリックし、[Banner] (バナー) ページを開きます。
2. [Display Restricted Service Banner] (制限付きサービス バナーを表示する) チェック ボックスをオンにし、この機能を有効にします。

3. ユーザがセキュリティ バナーに同意してからでないとログイン プロセスを続行できないようにするには、[Require Acceptance of Restricted Service Banner] (制限付きサービス バナーに対する同意を義務付ける) チェック ボックスをオンにします。ユーザがセキュリティ バナーに同意するには、チェック ボックスをオンにします。この設定を有効にしない場合、ユーザがログインした後にセキュリティ バナーが表示されるだけであり、ユーザがセキュリティ バナーに同意する必要はありません。
4. 必要があれば、バナー タイトルをカスタマイズします。この情報は、バナーの一部としてユーザに対して表示されます。最大 64 文字まで使用できます。
5. [Restricted Services Banner Message] (制限付きサービス バナー メッセージ) ボックス内のテキストをカスタマイズします。入力できるテキストは最大 6,000 文字です。直接入力する方法と、テキスト ファイルからアップロードする方法があります。次のいずれかの手順を実行します。
   a. このボックス内のテキストを手動で編集します。[OK] をクリックします。
   b. .txt ファイル内のテキストをアップロードします。具体的には、[Restricted Services Banner File] (制限付きサービス バナー ファイル) を選択し、[Browse] (参照) をクリックしてファイルを探し、アップロードします。[OK] をクリックします。ファイルがアップロードされると、そのファイル内のテキストが [Restricted Services Banner Message] (制限付きサービス バナー メッセージ) ボックスに表示されます。

注:ローカル ポートからテキスト ファイルをアップロードすることはできません。



保守

[Audit Log] (監査ログ)

KX III のシステム イベントに関するログが作成されます。監査ログは最大で約 2K 分のデータを保持でき、これを超えると最も古いエントリから上書きされます。監査ログのデータが失われないようにするには、syslog サーバまたは SNMP マネージャにデータをエクスポートします。syslog サーバまたは SNMP マネージャは、[Device Settings] (デバイス設定) の [Event Management] (イベント管理) ページから設定します。 監査ログおよび Syslog でキャプチャされる内容については、「***監査ログおよび Syslog でキャプチャされるイベント*** 『*358*p. 』」を参照してください。

▶ KX III の監査ログを表示するには

1. [Maintenance] (保守) メニューの [Audit Log] (監査ログ) をクリックします。[Audit Log] (監査ログ) ページが開きます。

[Audit Log] (監査ログ) ページでは、日時順にイベントが表示されます (最も新しいイベントが先頭に表示されます)。監査ログに含まれる情報は次のとおりです。

- [Date] (日時): イベントが発生した日時 (24 時間形式)。
- [Event] (イベント): [Event Management] (イベント管理) ページに一覧表示されるイベント名。
- [Description] (説明): イベントの詳細な説明。

▶ 監査ログを保存するには

注: 監査ログの保存は KX III リモート コンソールでのみ実行できます。KX III ローカル コンソールでは実行できません。

---

1. [Save to File] (ファイルに保存) をクリックします。[Save File] (ファイルに保存) ダイアログ ボックスが開きます。
2. ファイル名と保存先フォルダを選択し、[Save] (保存) をクリックします。監査ログが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。

▶ 監査ログのページ間を移動するには

- [Older] (古いログへ) リンクおよび [Newer] (新しいログへ) リンクを使用します。

[Device Information] (デバイス情報)

[Device Information] (デバイス情報) ページには、使用している KX III デバイスとコンピュータ インタフェース モジュール (CIM) に関する詳細情報が表示されます。これらの情報は、Raritan のテクニカル サポート部門に問い合わせをする際に役立ちます。

▶ KX III と CIM に関する情報を表示するには、以下の手順に従います。

- [Maintenance] (保守) メニューの [Device Information] (デバイス情報) をクリックします。[Device Information] (デバイス情報) ページが開きます。

使用している KX III に関する以下の情報が提供されます。

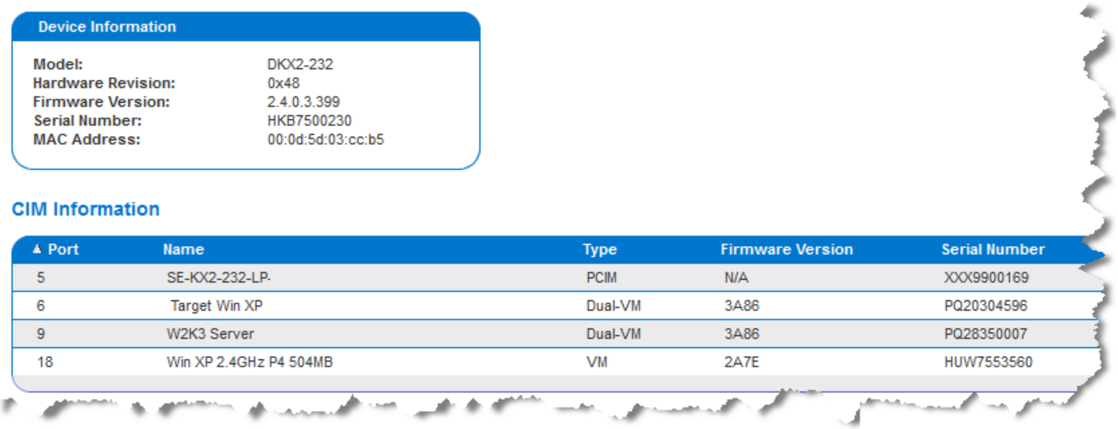
- [Model] (モデル)
- [Hardware Revision] (ハードウェア リビジョン)
- [Firmware Version] (ファームウェア バージョン)
- [Serial Number] (シリアル番号)
- [MAC Address] (MAC アドレス)

CIM に関して表示される情報は次のとおりです。

- [Port] (ポート) (番号)
- [Name] (名前)
- [Type of CIM] (CIM のタイプ) - DCIM、PCIM、ラック PDU、VM、DVM-DP、DVM-HDMI、DVM-DVI
- [Firmware Version] (ファームウェア バージョン)
- [Serial Number of the CIM] (CIM のシリアル番号) - サポートされている CIM からこの番号を直接入手できます。
  - P2CIM-PS2
  - P2CIM-APS2DUAL
  - P2CIM-AUSBDUAL
  - P2CIM-AUSB
  - P2CIM-SUN
  - P2CIM-SUSB
  - P2CIM-SER
  - DCIM-PS2
  - DCIM-USB
  - DCIM-USBG2
  - DCIM-SUN
  - DCIM-SUSB
  - D2CIM-VUSB

- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB

注:DCIM-USB、DCIM-PS2、DCIM-USB G2 の 各 CIM のシリアル番号の数字部分のみが表示されます。たとえば、XXX1234567 が表示されます。シリアル番号がフィールドで設定された CIM には、シリアル番号プレフィックス GN が表示されます。



バックアップと復元

[Backup/Restore] (バックアップ/復元) ページでは、KX III の設定情報をバックアップおよび復元できます。

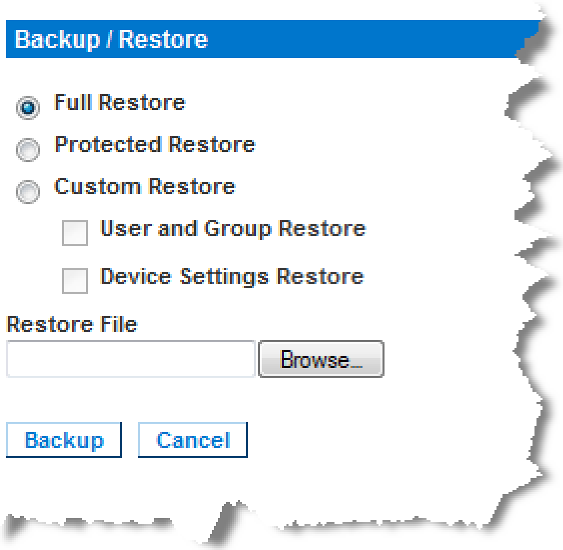
バックアップ/復元機能には、業務継続性を確保するというメリットに加え、時間節約効果もあります。

たとえば、使用中の KX III のユーザ設定情報をバックアップして別の KX III に復元することにより、その復元先 KX III をすぐに使用できるようになります。

また、1 台の KX III をセットアップし、その設定情報を複数台の KX III にコピーすることもできます。

[Backup/Restore] (バックアップ/復元) ページを開くには

- [Maintenance] (保守) メニューの [Backup/Restore] (バックアップ/復元) をクリックします。[Backup/Restore] (バックアップ/復元) ページが開きます。



注:バックアップ処理では、常にシステム全体がバックアップされます。復元処理では、全体を復元するか一部を復元するかをユーザが選択できます。

Internet Explorer 7 以降を使用している場合、KX III をバックアップするには、以下の手順に従います。

1. [Backup] (バックアップ) をクリックします。[Open] (開く) ボタンを含む [File Download] (ファイルのダウンロード) ダイアログ ボックスが開きます。[Open] (開く) をクリックしないでください。

IE 7 (以降) では、ファイルを開くデフォルトのアプリケーションとして IE が使用されるため、ファイルを開くか、または保存するように求められます。これを回避するには、ファイルを開くために使用されるデフォルトのアプリケーションをワードパッド® に変更する必要があります。

2. このためには、以下の手順に従います。
   a. バックアップ ファイルを保存します。バックアップ ファイルが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。
   b. 保存されたら、ファイルを探して右クリックします。[プロパティ] を選択します。
   c. [全般] タブで [変更] をクリックし、[WordPad] を選択します。

KX III を復元するには

警告: 使用している KX III を旧バージョンに復元する場合、注意が必要です。バックアップ時点で設定されていたユーザ名とパスワードが復元されます。つまり、バックアップ時点での管理者のユーザ名とパスワードを覚えていない場合、KX III からロックアウトされます。

また、バックアップ時点で現在と異なる IP アドレスを使用していた場合、その IP アドレスも同様に復元されます。IP アドレスの割り当てに DHCP を使用している場合、ローカル ポートにアクセスして復元後の IP アドレスを調べる必要があります。

1. 実行する復元処理のタイプを選択します。
   - [Full Restore] (完全復元): システム全体を復元します。この復元タイプの主な用途は、一般的なバックアップ/復元処理です。
   - [Protected Restore] (部分復元): デバイス固有情報 (例: IP アドレス、名前) 以外のすべての情報が復元されます。この復元タイプの用途としては、1 台の KX III をセットアップし、その設定情報を複数台の KX III にコピーするケースなどが考えられます。
   - [Custom Restore] (カスタム復元): この復元タイプを選択した場合、[User and Group Restore] (ユーザとグループの復元) チェック ボックスと [Device Settings Restore] (デバイス設定の復元) チェック ボックスのいずれか一方または両方をオンにすることができます。

- [User and Group Restore] (ユーザとグループの復元): このチェック ボックスをオンにした場合、ユーザ情報とグループ情報だけが復元されます。証明書および秘密鍵ファイルは*復元されません*。別の KX III 上でユーザ情報をセットアップする際に便利です。
- [Device Settings Restore] (デバイス設定の復元): このチェック ボックスをオンにした場合、デバイス設定情報 (例: 関連電源、USB プロファイル、ブレード シャーシ関連の設定パラメータ、ポート グループの割り当て) だけが復元されます。デバイス情報をコピーする際に便利です。

2. [Browse] (参照) をクリックします。[Choose file] (ファイルを選択) ダイアログ ボックスが開きます。
3. 適切なバックアップ ファイルを探して選択し、[Open] (開く) をクリックします。選択したファイルが [Restore File] (復元ファイル) ボックスに表示されます。
4. [Restore] (復元) をクリックします。選択した復元タイプに基づいて、設定情報が復元されます。

[USB Profile Management] (USB プロファイルの管理)

[USB Profile Management] (USB プロファイル管理) ページでは、Raritan のテクニカル サポート部門から提供されたカスタム プロファイル情報をアップロードできます。これらのプロファイルは、標準プロファイルがターゲット サーバ構成のニーズに対応していない場合にそのニーズに対応できるよう、設計されています。Raritan のテクニカル サポートは、カスタム プロファイルを提供し、ターゲット サーバ固有のニーズに対する解決策をお客様と一緒に探します。

▶ [USB Profile Management] (USB プロファイル管理) ページを開くには

- [Maintenance] (保守) メニューの [USB Profile Management] (USB プロファイル管理) をクリックします。[USB Profile Management] (USB プロファイル管理) ページが開きます。

▶ カスタム プロファイル情報を KX III にアップロードするには

1. [Browse] (参照) をクリックします。[Choose file] (ファイルを選択) ダイアログ ボックスが開きます。
2. 適切なカスタム プロファイル ファイルを探して選択し、[Open] (開く) をクリックします。選択したファイルが [USB Profile File] (USB プロファイル ファイル) ボックスに表示されます。
3. [Upload] (アップロード) をクリックします。カスタム プロファイル情報がアップロードされ、プロファイル一覧に表示されます。

注:アップロード処理中にエラーまたは警告が表示された場合 (例: 既存のカスタム プロファイルが上書きされる場合)、アップロード処理を続行するには [Upload] (アップロード)、アップロード処理をキャンセルするには [Cancel] (キャンセル) をクリックします。

▶ カスタム プロファイル情報を KX III から削除するには

1. 削除するカスタム プロファイルのチェック ボックスをオンにします。
2. [Delete] (削除) をクリックします。カスタム プロファイル情報が削除され、プロファイル一覧に表示されなくなります。

アクティブになっているカスタム プロファイルでも削除できます。ただしその場合、確立されていた仮想メディア セッションがすべて終了します。

プロファイル名の競合を処理する

ファームウェアをアップグレードしたとき、カスタム USB プロファイルと標準 USB プロファイルの名前が競合することがあります。たとえば、あるカスタム プロファイルを作成して標準プロファイル リストに組み込んでおり、ファームウェアのアップグレード時に同名の USB プロファイルがダウンロードされた場合などです。

この場合、既存のカスタム プロファイルの名前に old_ というプレフィックスが付加されます。たとえば、GenericUSBProfile5 という名前のカスタム プロファイルが存在しており、かつ、ファームウェアのアップグレード時に同名のプロファイルがダウンロードされた場合、既存のカスタム プロファイルの名前が old_GenericUSBProfile5 に変更されます。

必要に応じて、既存のプロファイルを削除できます。詳細については、「*USB プロファイルの管理* 『*195*p. の"*[USB Profile Management] (USB プロファイルの管理)*"参照 』」を参照してください。

CIM アップグレード

この項で説明する手順に従って、KX III のメモリに格納されているファームウェア バージョンを基に CIM をアップグレードします。一般に、[Firmware Upgrade] (ファームウェアのアップグレード) ページを使用してデバイスのファームウェアをアップグレードする場合、すべての CIM がアップグレードされます。

▶ KX III のメモリを使用して CIM をアップグレードするには

1. [Maintenance] (保守) メニューの [CIM Firmware Upgrade] (CIM ファームウェアのアップグレード) をクリックします。[CIM Upgrade from] (CIM のアップグレード) ページが開きます。

[Port] (ポート)、[Name] (名前)、[Type] (タイプ)、[Current CIM Version] (現在の CIM バージョン)、[Upgrade CIM Version] (アップグレード先の CIM バージョン) の各列に情報が表示されるので、各 CIM を簡単に識別できます。

2. アップグレードしたい各 CIM の [Selected] (選択) チェック ボックスをオンにします。
3. [Upgrade] (アップグレード) をクリックします。アップグレードしてもよいかどうかを確認するダイアログ ボックスが開きます。
4. [OK] をクリックしてアップグレード処理を続行します。アップグレード処理中は、進行状況バーが表示されます。アップグレード処理には、CIM ごとに最長で約 2 分かかります。

KX III ファームウェアのアップグレード

[Firmware Upgrade] (ファームウェアのアップグレード) ページを使用して、KX III および接続するすべての CIM のファームウェアをアップグレードします。このページは、KX III リモート コンソールでのみ使用できます。

[Firmware Upgrade] (ファームウェアのアップグレード)

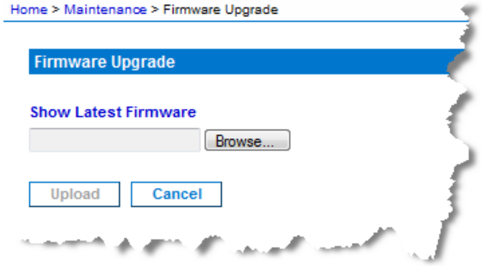
重要: アップグレード処理中に、KX III の電源を切断したり CIM を取り外したりしないでください。KX III または CIM が損傷するおそれがあります。

▶ KX III をアップグレードするには

1. *Raritan の Web サイト http://www.raritan.com* の [Firmware Upgrades] (ファームウェアのアップグレード) ページで、適切な Raritan ファームウェア配布ファイル (.rfp ファイル) を探してダウンロードします。
2. そのファイルを解凍します。アップグレードを実行する前に、解凍したファイルに記載されている指示をすべてお読みください。

   注:アップグレードを実行する前に、そのファームウェア配布ファイルをローカル PC にコピーしておいてください。また、そのファームウェア配布ファイルをネットワーク ドライブからロードしないでください。

3. [Maintenance] (保守) メニューの [Firmware Upgrade] (ファームウェアのアップグレード) をクリックします。[Firmware Upgrade] (ファームウェアのアップグレード) ページが開きます。



4. [Browse] (参照) をクリックし、ファームウェア配布ファイルを解凍したフォルダに移動します。
5. [Firmware Upgrade] (ファームウェアのアップグレード) ページの [Upload] (アップロード) をクリックします。

   アップグレードとバージョン番号に関する情報が、確認のために表示されます。CIM 情報を表示するよう指定した場合は、その情報も表示されます。

   注:この時点で接続していたユーザはログオフされ、新たにログオンしようとしたユーザはブロックされます。

   ---

6. [Upgrade] (アップグレード) をクリックします。アップグレード処理が完了するまで待機します。アップグレード処理中は、ステータス情報および進行状況バーが表示されます。アップグレード処理が完了すると、KX III が再起動します。再起動が完了するとビープ音が 1 回鳴ります。
7. 指示に従ってブラウザを終了し、約 5 分待ってから再度 KX III にログオンします。

アップグレード履歴

KX III および接続されている CIM に対して実行されたアップグレード処理に関する情報を表示できます。

アップグレード履歴を表示するには、以下の手順に従います。

- ［保守］メニューの［アップグレード履歴］をクリックします。［アップグレード履歴］ページが開きます。

実行された KX III アップグレード処理に関する情報、アップグレード処理の最終ステータス、アップグレード処理の開始日時と終了日時、および、アップグレード前と現在のファームウェア バージョンが表示されます。CIM に関する情報を表示するには、［CIM］列の［表示］リンクをクリックします。表示される CIM 情報は次のとおりです。

- [タイプ]: CIM のタイプ。
- [ポート]: CIM が接続されているポート。
- [ユーザ]: アップグレード処理を実行したユーザ。
- [IP]: IP アドレス。
- [開始日時]: アップグレード処理の開始日時。
- [終了日時]: アップグレード処理の終了日時。
- [前のバージョン]: アップグレード前の CIM ファームウェア バージョン。
- [アップグレード バージョン]: 現在の CIM ファームウェア バージョン。
- [CIM]: アップグレードされた CIM。
- [結果]: アップグレード処理の結果（成功または失敗）。

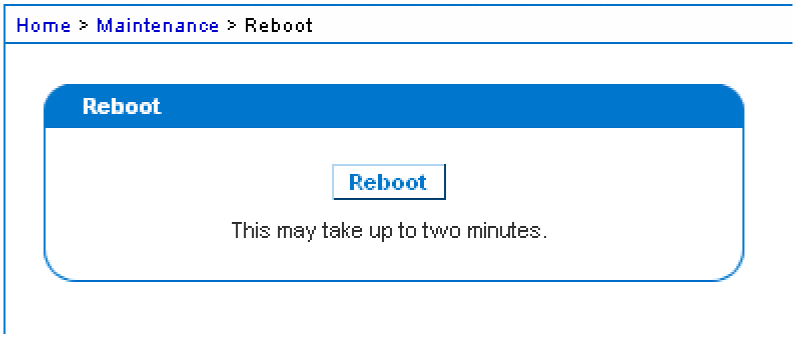
KX III の再起動

[Reboot]（再起動）ページでは、KX III を安全に再起動できます。再起動する場合、このページから行うことを推奨します。

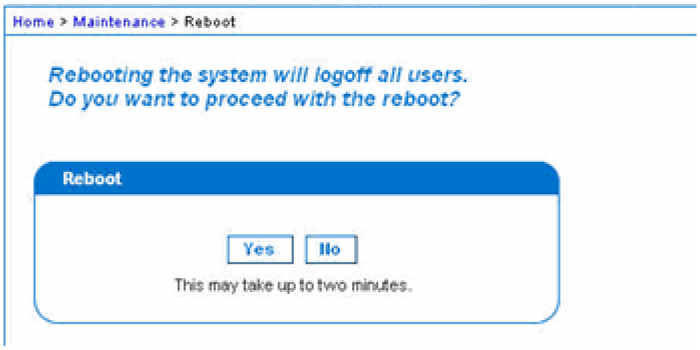
重要: すべての KVM 接続およびシリアル接続が切断され、また、すべてのユーザがログオフされます。

KX III を再起動するには

1. [Maintenance] (保守) メニューの [Reboot] (再起動) をクリックします。[Reboot] (再起動) ページが開きます。



2. [Reboot] (再起動) をクリックします。再起動してもよいかどうかを確認するダイアログ ボックスが開きます。[Yes] (はい) をクリックし、再起動処理を続行します。



CC-SG 管理の終了

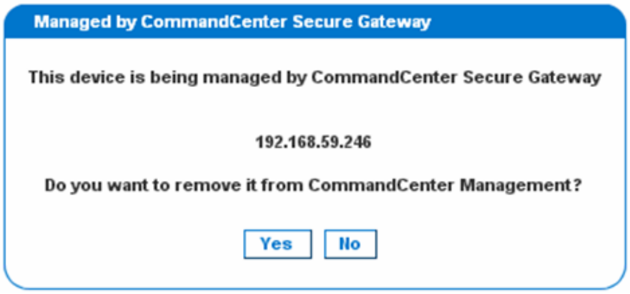
KX III が CommandCenter Secure Gateway (CC-SG) の管理下にあるのに、KX III に直接アクセスしようとすると、KX III が CC-SG の管理下にあることを示すメッセージが表示されます。

KX III が CC-SG の管理下にあるが、指定タイムアウト間隔 (通常は 10 分) が経過した後に CC-SG と KX III の間の接続が切断された場合、KX III コンソールから CC-SG 管理セッションを終了できます。

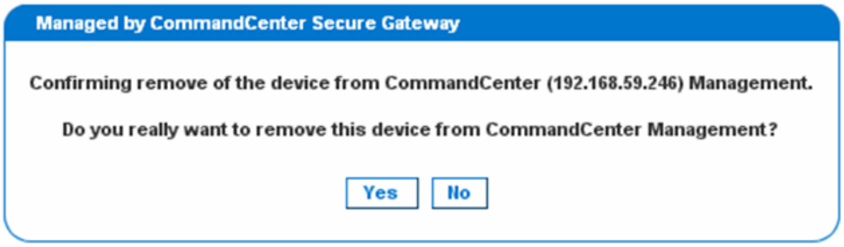
注:KX III を CC-SG の管理対象から除外するには、適切な権限が必要です。また、KX III が現在 CC-SG の管理下にない場合、[Maintenance] (保守) メニューの [Stop CC-SG Management] (CC-SG の管理対象から除外する) コマンドは無効になります。

▶ **KX III を CC-SG の管理対象から除外するには、以下の手順に従います。**

1. [Maintenance] (保守) メニューの [Stop CC-SG Management] (CC-SG の管理対象から除外する) をクリックします。"KX III が CC-SG の管理下にある" という内容のメッセージが表示されます。また、KX III を CC-SG の管理対象から除外するためのボタンも表示されます。



2. [Yes] (はい) をクリックし、KX III を CC-SG の管理対象から除外する処理を開始します。KX III を CC-SG の管理対象から除外してもよいかどうかを確認するためのメッセージが表示されます。



3. [Yes] (はい) をクリックし、KX III を CC-SG の管理対象から除外します。KX III が CC-SG の管理対象から除外されると、処理完了メッセージが表示されます。

診断

[Network Interface] (ネットワーク インタフェース) ページ

KX III では、ネットワーク インタフェースのステータス情報を確認できます。

ネットワーク インタフェースに関する情報を表示するには

- [Diagnostics] (診断) メニューの [Network Interface] (ネットワーク インタフェース) をクリックします。[Network Interface] (ネットワーク インタフェース) ページが開きます。

表示される情報は次のとおりです。

- Ethernet インタフェースが稼動しているかどうか。
- ゲートウェイから ping できるかどうか。
- 現在アクティブな LAN ポート。

これらの情報を更新するには

- [Refresh] (更新) をクリックします。

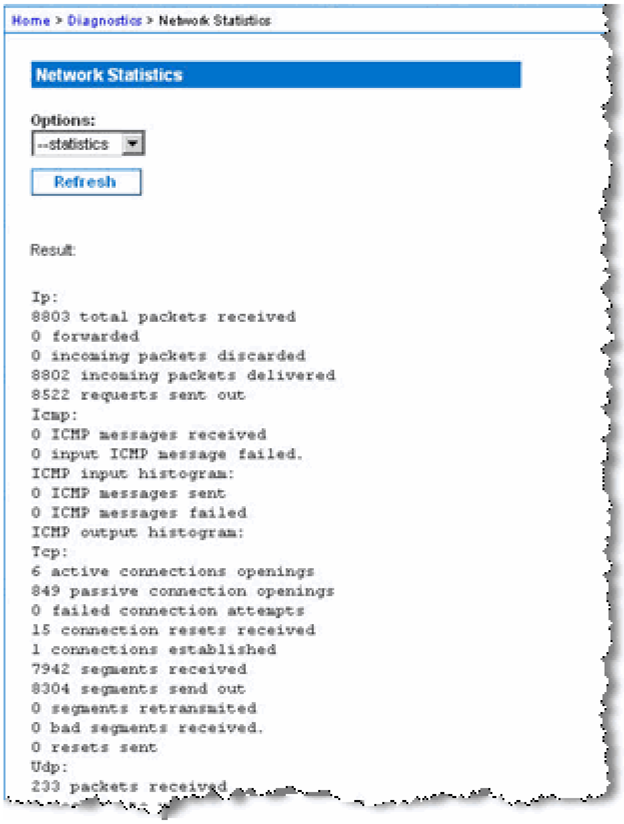
[Network Statistics] (ネットワーク統計) ページ

KX III では、ネットワーク インタフェースに関する統計情報を表示できます。

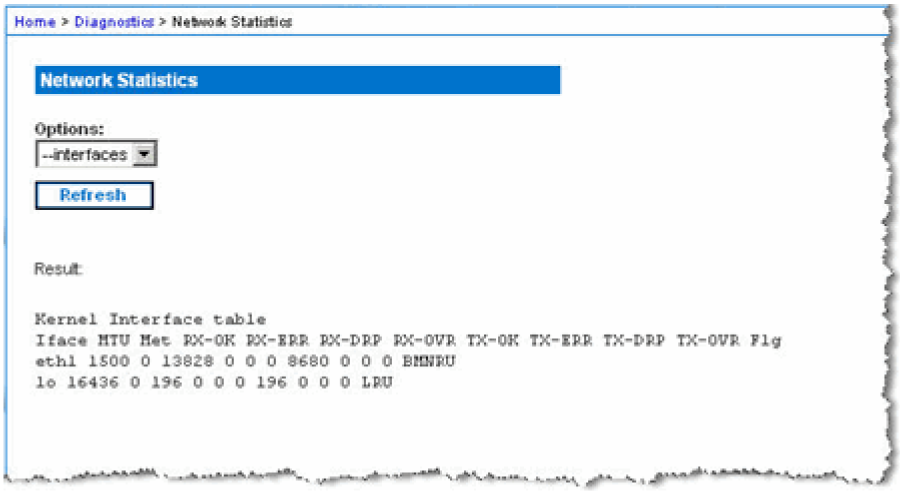
ネットワーク インタフェースに関する統計情報を表示するには

1. [Diagnostics] (診断) メニューの [Network Statistics] (ネットワーク統計) をクリックします。[Network Statistics] (ネットワーク統計) ページが開きます。
2. [Options] (オプション) ボックスの一覧で値を選択します。

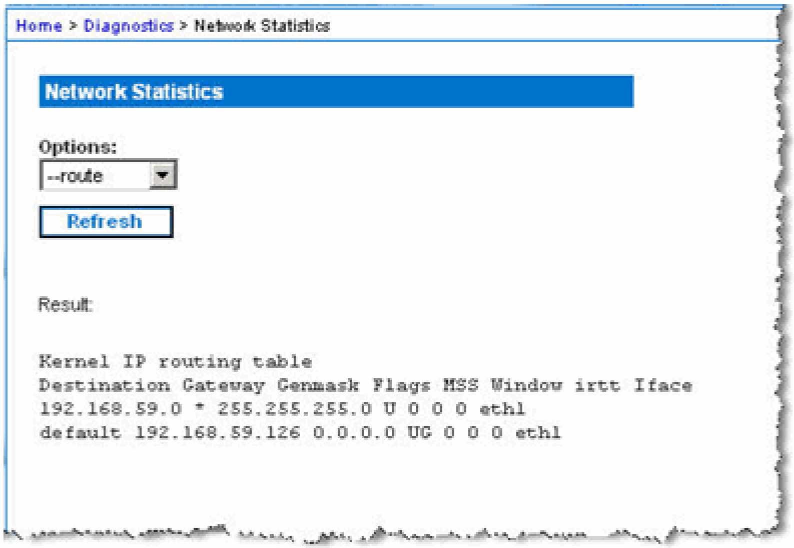
- [Statistics] (統計): 次に示すような情報が表示されます。



- [Interfaces] (インタフェース): 次に示すような情報が表示されます。



- [Route] (経路): 次に示すような情報が表示されます。



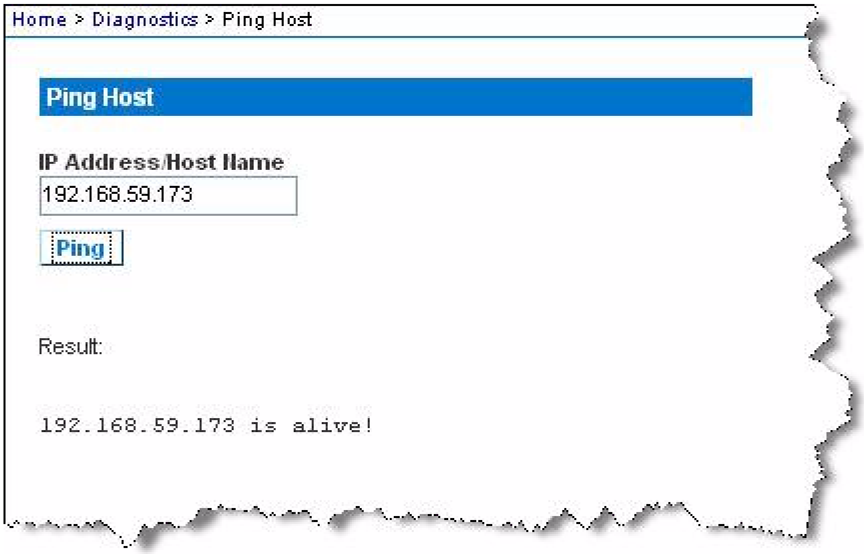
3. [Refresh] (更新) をクリックします。[Options] (オプション) ボックスの一覧で選択した値に応じた情報が、[Result] (結果) フィールドに表示されます。

[ホストに ping する] ページ

ping は、特定のホストまたは IP アドレスが IP ネットワーク上で接続可能であるかどうかをテストするためのネットワーク コマンドです。[Ping Host] (ホストに ping する) ページでは、ターゲット サーバまたは別の KX III がアクセス可能であるかどうかを調べることができます。

▶ ホストに ping するには

1. [Diagnostics] (診断) メニューの [Ping Host] (ホストに ping する) をクリックします。[Ping Host] (ホストに ping する) ページが開きます。



2. [IP Address/Host Name] (IP アドレス/ホスト名) ボックスに IP アドレスまたはホスト名を入力します。

   注: ホスト名は 232 文字以内で指定してください。

3. [Ping] (ping) をクリックします。ping の実行結果が [Result] (結果) フィールドに表示されます。

[Trace Route to Host (ホストへのルートの追跡)] ページ

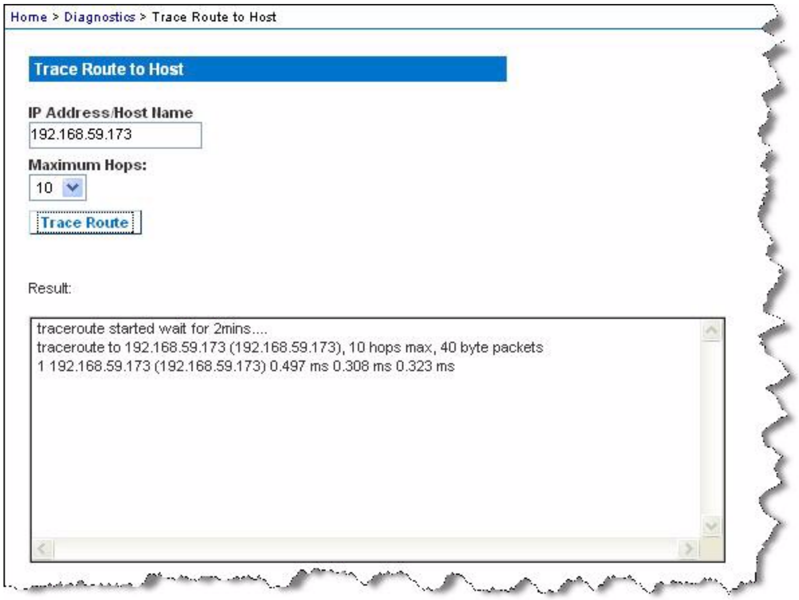
trace route (ルートの追跡) は、指定したホスト名または IP アドレスへのルートを調べるためのネットワーク ツールです。

▶ ホストへのルートを追跡するには、次の手順に従います。

1. [Diagnostics (診断)] > [Trace Route to Host (ホストへのルートの追跡)] を選択します。[Trace Route to Host (ホストへのルートの追跡)] ページが表示されます。
2. [IP Address/Host Name (IP アドレス/ホスト名)] フィールドに IP アドレスまたはホスト名を入力します。

注: ホスト名は最大 232 文字です。

3. ドロップダウン リストから最大ホップ数を選択します (5 刻みで 5 ～ 50)。
4. [Trace Route (ルートの追跡)] をクリックします。指定したホスト名または IP アドレスに対して、trace route コマンドが、指定した最大ホップ数以内で実行されます。trace route の実行結果が [Result (結果)] フィールドに表示されます。



KX III 診断

注: これは、Raritan フィールド エンジニアが使用するためのページです。Raritan のテクニカル サポート部門から指示された場合に限り、ユーザも使用できます。

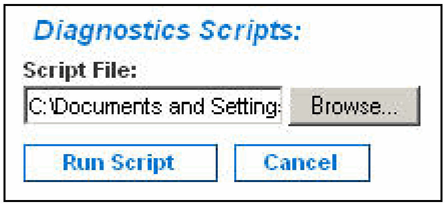
[KX III 診断] ページでは、診断情報を KX III からクライアント コンピュータにダウンロードできます。このページでは、次の 2 種類の処理を行うことができます。

- 重大エラー デバッグ セッション中に、Raritan のテクニカル サポート部門から提供された特別な診断スクリプトを実行する。このスクリプトは、KX III にアップロードされ、実行されます。このスクリプトの実行が完了した後、[ファイルに保存] 機能を使用して診断メッセージをダウンロードできます。
- 診断メッセージのスナップショットに対するデバイス診断ログを、KX III からクライアント コンピュータにダウンロードする。このダウンロードされたデバイス診断ログは暗号化ファイルであり、Raritan のテクニカル サポート部門に送信されます。このファイルを解析できるのは Raritan だけです。

注: このページを開くことができるのは、管理者権限を持つユーザだけです。

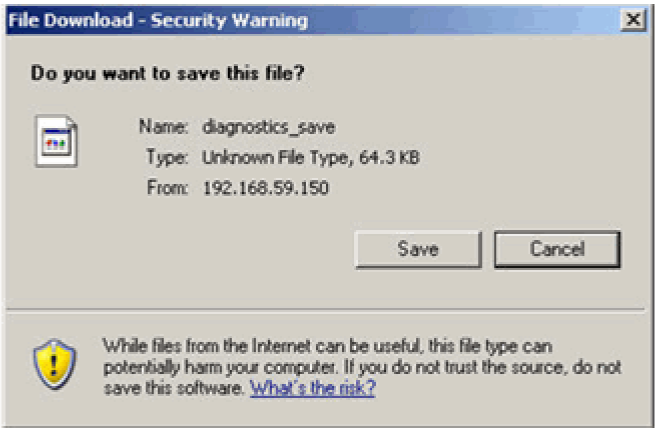
KX III のシステム診断を実行するには、以下の手順に従います。

1. [診断] メニューの [KX III 診断] をクリックします。[KX III 診断] ページが開きます。
2. Raritan のテクニカル サポート部門から電子メールで受け取った診断スクリプト ファイルを実行するため、次の手順を実行します。
   a. Raritan から提供されている診断スクリプト ファイルを入手します。圧縮されている場合は解凍します。
   b. [参照] をクリックします。[ファイルを選択] ダイアログ ボックスが開きます。
   c. 診断スクリプト ファイルを探して選択します。
   d. [開く] をクリックします。診断スクリプト ファイルの名前が [スクリプト ファイル] ボックスに表示されます。



   e. [スクリプトを実行] をクリックします。この診断スクリプト ファイルを Raritan のテクニカル サポート部門に送信します。

3. 診断ファイルを作成して Raritan のテクニカル サポート部門に送信するため、次の手順を実行します。
   a. ［ファイルに保存］をクリックします。［ファイルのダウンロード］ダイアログ ボックスが開きます。



   b. ［保存］をクリックします。［名前を付けて保存］ダイアログ ボックスが開きます。
   c. 保存先フォルダに移動し、［保存］をクリックします。
   d. Raritan のテクニカル サポート部門の指示に従って、このファイルを E メールで送信します。

KX III ローカル コンソール

KX III では、ローカル ポート経由でローカルにアクセスおよび管理を行うことができます。KX III には、ローカル コンソールを介してアクセスできます。

KX III リモート コンソールから実行される大半の管理機能は、ローカル コンソールからも実行できます。

このセクションでは、管理者タスクについて具体的に説明します。ローカル コンソールから実行されるエンド ユーザ タスクについては、ユーザ ヘルプを参照してください。

セキュリティと認証

KX III ローカル コンソールを使用するには、まず有効なユーザ名とパスワードで認証を受ける必要があります。KX III には認証機能とセキュリティ機能が備わっています。これらの機能は、ネットワークから接続するユーザとローカル ポートから接続するユーザの両方に対して有効です。ユーザは、どちらの方法で接続する場合でも、アクセス権限を持っているサーバにしかアクセスできません。サーバ アクセスとセキュリティに関する設定情報を指定する手順については、「ユーザ管理」を参照してください。

KX III が外部認証サービス（LDAP/LDAPS、RADIUS、または Active Directory）を使用するように設定されている場合、ユーザが KX III ローカル コンソールを使用して接続する際でも、外部認証サービスによって認証が行われます。

注: KX III ローカル コンソールを使用して接続しようとするユーザに対して認証を行わないように、設定することもできます。ただし、この方法は安全な環境でのみ使用することを推奨します。

KX III ローカル コンソールを使用するには

1. キーボード、マウス、およびモニタを、KX III の背面にあるローカル ポートに接続します。
2. KX III を起動します。KX III ローカル コンソール画面が表示されます。

ローカル コンソールからの KX III ローカル ポートの設定

標準ローカル ポートを設定するには、リモート コンソールで [Port Configuration]（ポート設定）ページを使用するか、ローカル コンソールで [Local Port Settings]（ローカル ポート設定）ページを使用します。

[Local Port Settings]（ローカル ポート設定）ページでは、KX III ローカル コンソールに関するさまざまな設定値をカスタマイズできます。たとえば、キーボード、ホットキー、画面切り替え遅延、省電力モード、画面解像度設定、ローカル ユーザ認証などに関する設定値をカスタマイズできます。

注: これらのページを使用できるのは、管理者権限を持つユーザだけです。

注:[Local Port Settings]（ローカル ポート設定）ページで設定を変更すると、作業中のブラウザが再起動する場合があります。変更時にブラウザが再起動する設定については、以下の手順に示されています。

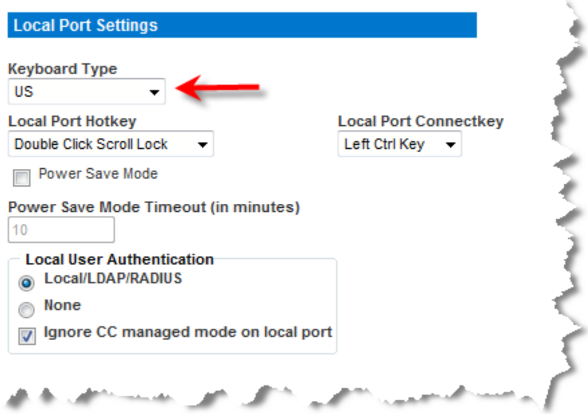
ローカル ポートに関する設定値をカスタマイズするには

1. [Device Settings]（デバイス設定）メニューの [Local Port Settings]（ローカル ポート設定）をクリックします。[Local Port Settings]（ローカル ポート設定）ページが開きます。

ローカル コンソールのキーボード タイプの選択

1. [Keyboard Type] (キーボード タイプ) ドロップダウン リストでキーボード タイプを選択します。選択できる項目は次のとおりです。

   この設定を変更すると、ブラウザが再起動します。



- [US] (アメリカ英語)
- [US/International] (アメリカ英語/国際)
- [United Kingdom] (イギリス英語)
- [French (France)] (フランス語 (フランス))
- [German (Germany)] (ドイツ語 (ドイツ))
- [German (Switzerland)] (ドイツ語 (スイス))
- [Simplified Chinese] (簡体字中国語)
- [Traditional Chinese] (繁体字中国語)
- [Dubeolsik Hangul (Korean)] (Dubeolsik ハングル (韓国))
- [JIS (Japanese Industry Standard)] (JIS (日本工業規格))
- [Portuguese (Portugal)] (ポルトガル語 (ポルトガル))
- [Norwegian (Norway)] (ノルウェー語 (ノルウェー))
- [Swedish (Sweden)] (スウェーデン語 (スウェーデン))
- [Danish (Denmark)] (デンマーク語 (デンマーク))
- [Belgian (Belgium)] (ベルギー語 (ベルギー))
- ハンガリー語
- スペイン語
- イタリア語
- スロベニア語

注:中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。

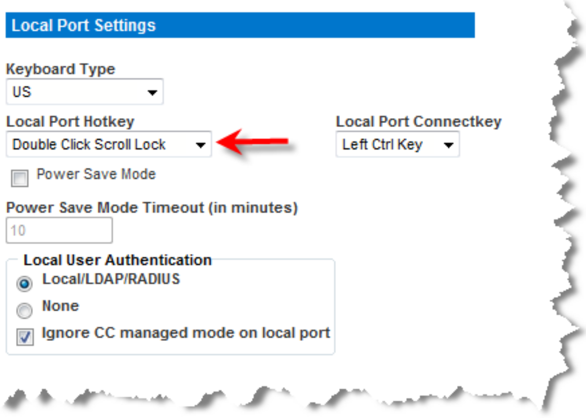
注:トルコ語のキーボードを使用している場合は、Active KVM Client (AKC) を介してターゲット サーバに接続する必要があります。他の Raritan クライアントではサポートされていません。

ローカル ポート ホットキーの選択

1. [Local Port Hotkey] (ローカル ポート ホットキー) ボックスの一覧でローカル ポート ホットキーを選択します。ローカル ポート ホットキーは、ターゲット サーバの画面が表示されているときに KX III ローカル コンソールの画面に戻す際に使用します。デフォルト値は [Double Click Scroll Lock] (Scroll Lock キーを 2 回押す) ですが、他のキー組み合わせを選択することもできます。

ホットキー	説明
Scroll Lock キーをすばやく 2 回押す	Scroll Lock キーをすばやく 2 回押します。
[Double Click Num Lock] (Num Lock キーを 2 回押す)	Num Lock キーをすばやく 2 回押します。

ホットキー	説明
[Double Click Caps Lock] (Caps Lock キーを 2 回押す)	Caps Lock キーをすばやく 2 回押します。
[Double Click Left Alt key] (左 Alt キーを 2 回押す)	左 Alt キーをすばやく 2 回押します。
[Double Click Left Shift key] (左 Shift キーを 2 回押す)	左 Shift キーをすばやく 2 回押します。
[Double Click Left Ctrl key] (左 Ctrl キーを 2 回押す)	左 Ctrl キーをすばやく 2 回押します。



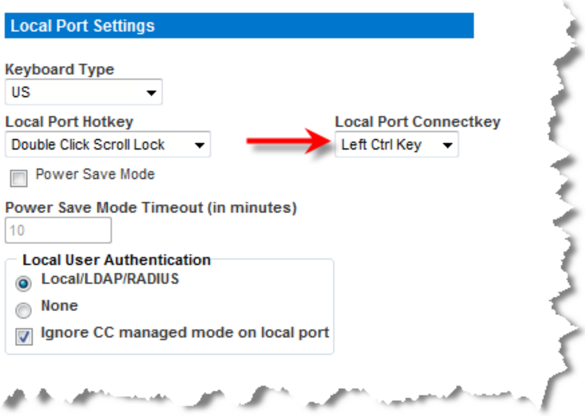
ローカル ポート接続キーの選択

1. ローカル ポート接続キーを選択します。接続キーは、あるターゲット サーバにアクセスしているときに別のターゲット サーバに切り替える際に使用します。

   その後ホットキーを使用して、そのターゲット サーバの画面から KX III ローカル コンソールの画面に戻すことができます。

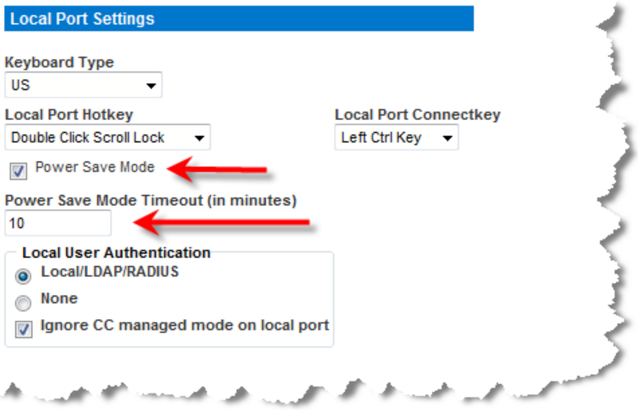
   接続キーを設定すると、ナビゲーション パネルに表示されるので、すぐにわかります。接続キー組み合わせの例については、「*接続キーの例* 『*299*p. 』」を参照してください。

接続キーは、標準型サーバとブレード筐体のどちらに対しても機能します。



省電力機能の設定 (オプション)

1. 省電力機能を利用する場合、次の手順を実行します。
   a. [Power Save Mode] (省電力モード) チェック ボックスをオンにします。
   b. [Power Save Mode Timeout (in minutes)] (省電力モードのタイムアウト (分)) ボックスに、省電力モードに移行するまでの時間 (単位: 分) を入力します。



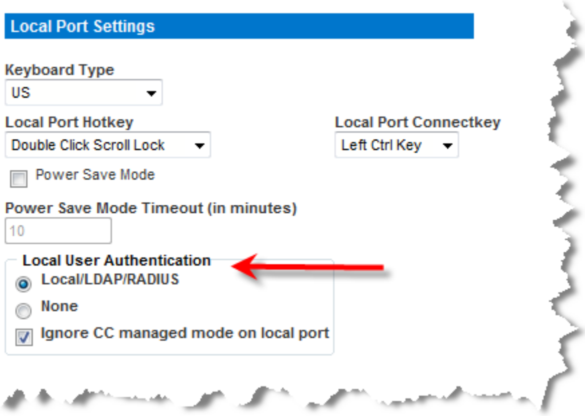
ローカル ユーザ認証の選択

1. [Local User Authentication] (ローカル ユーザ認証) でローカル ユーザ認証タイプを選択します。
   - [Local/LDAP/RADIUS] (ローカル/LDAP/RADIUS)これは推奨オプションです。

     認証の詳細については、「リモート認証」を参照してください。

- 特別なアクセス用ソフトウェアをインストールする必要はありません。KX III ローカル コンソールからのアクセスに対して認証は行われません。

  このオプションは、安全な環境でのみ選択することを推奨します。

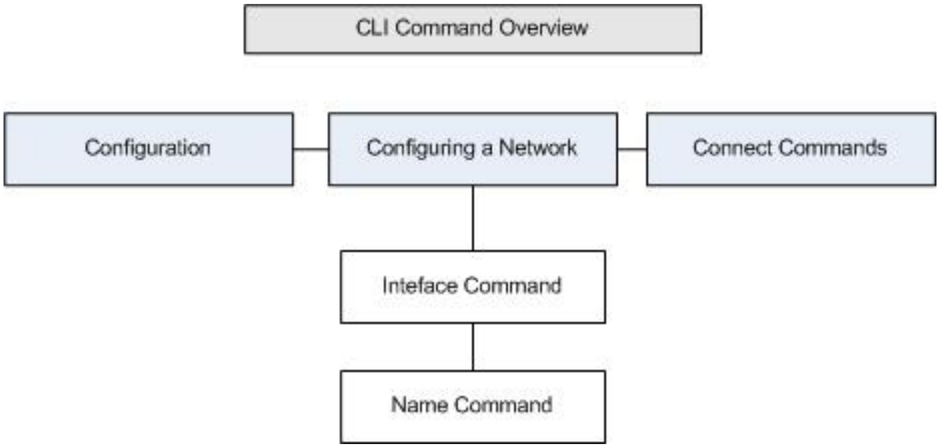


コマンド ライン インタフェース (CLI)

概要

KX III のネットワーク インタフェースを設定する権限や診断処理を実行する権限を持っている場合、コマンド ライン インタフェース (CLI) を使用してそれらの処理を実行できます。

次の図に CLI コマンドの概要を示します。コマンドの一覧については、「*CLI コマンド* 『*219*p. 』」を参照してください。この一覧には、各コマンドの説明、および、各コマンドの記述例が書かれている項へのリンクがあります。



top、history、log off、quit、show、help の各コマンドは、この図のどの CLI レベルからでも使用できます。

CLI を使用しての KX III へのアクセス

次の方法のいずれかを使用して、KX III にアクセスします。

- IP 接続を介した SSH (Secure Shell)

複数の SSH クライアントを使用可能で、次の場所から取得できます。

- Putty: *http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/*参照
- ssh.com の SSH クライアント: *www.ssh.com http://www.ssh.com* 参照
- Applet SSH Client: *www.netspace.org/ssh http://www.netspace.org/ssh* 参照
- OpenSSH Client: *www.openssh.org http://www.openssh.org* 参照

KX III への SSH 接続

SSHv2 をサポートする Secure Shell (SSH) クライアントを使用して、KX III に接続します。[Devices Services] (デバイス サービス) ページで SSH 接続を有効にしておく必要があります。

注: セキュリティ上の理由により、SSHv1 接続は KX III でサポートされていません。

Windows PC から SSH で接続する

Windows® PC から SSH セッションを開くには

1. SSH クライアント ソフトウェアを起動します。
2. KX III サーバの IP アドレスを入力します (例: 「192.168.0.192」)。
3. SSH を選択します。SSH では、デフォルトの設定ポート 22 が使用されます。
4. [Open] (開く) をクリックします。

`login as:` (ログイン) プロンプトが表示されます。

「*ログイン* 『*216*p. 』」を参照してください。

UNIX/Linux ワークステーションから SSH で接続する

UNIX®/Linux® ワークステーションから SSH セッションを開き、ユーザ admin としてログオンするため、次のコマンドを入力します。

```
ssh -l admin 192.168.30.222
```

パスワードの入力を求めるプロンプトが表示されます。

「*ログイン* 『*216*p. 』」を参照してください。

ログイン

▶ **ログインするには、次のようにユーザ名 admin を入力します。**

1. admin としてログインします。
2. パスワードの入力を求めるプロンプトが表示されます。デフォルトパスワード（「*raritan*」）を入力します。

   歓迎メッセージが表示されます。これで、管理者としてログオンしたことになります。

次項「*CLI の画面操作* 『*216*p. 』」の内容を確認した後、初期設定処理を実行します。

CLI の画面操作

CLI を使用する前に、CLI の画面操作と構文について理解しておくことが重要です。また、CLI の使用を簡素化するキー入力の組み合わせについても、理解しておく必要があります。

コマンドのオート コンプリート

CLI にはオート コンプリート機能（コマンドの一部を入力すると、残りの部分が自動入力される機能）が備わっています。先頭の数文字を入力した後、Tab キーを押します。入力した文字列で始まるコマンドの候補が 1 つしかない場合、オート コンプリート機能によって残りの部分が自動入力されます。

- 入力した文字列で始まるコマンドの候補が見つからない場合、そのレベルに対する有効な入力候補が表示されます。
- 入力した文字列で始まるコマンドの候補が複数個見つかった場合、すべての入力候補が表示されます。

この場合、コマンドの続きを入力して候補が 1 つだけになるようにし、Tab キーを押してコマンドを自動入力します。

CLI 構文: ヒントとショートカット キー

ヒント

- コマンドは、アルファベット順に表示されています。
- コマンドでは、大文字と小文字は区別されません。
- パラメータ名は、アンダスコアを含まない 1 つの単語です。
- コマンドに対して引数を指定しない場合、そのコマンドに対する現在の設定値が指定されていると見なされます。
- コマンドの後ろに疑問符 (?) を指定した場合、そのコマンドに対するヘルプが表示されます。
- 縦線（|）は、任意指定または必須指定のキーワードまたは引数における、選択肢を意味します。

ショートカット

- 末尾のエントリを表示するには、上方向キーを押します。
- 最後に入力した文字を削除するには、Backspace キーを押します。
- 誤ったパラメータを入力した場合にコマンドを終了またはキャンセルするには、Ctrl キーを押しながら C キーを押します。
- コマンドを実行するには、Enter キーを押します。
- コマンドの入力中に残りの部分を自動入力するには、Tab キーを押します。たとえば、Admin Port > プロンプトで Conf と入力した後に Tab キーを押すと、Admin Port > Config > プロンプトが表示されます。

すべての CLI レベルで使用できるコマンド

次の表に、すべての CLI レベルで使用できるコマンドを示します。これらのコマンドは、CLI の画面操作にも役立ちます。

コマンド	説明
top	CLI 階層の最上位レベル、つまり username プロンプトに戻ります。
history	KX III の CLI で入力した最後の 200 個のコマンドが表示されます。
help	CLI 構文の概要が表示されます。
quit	1 レベル上に戻ります。
logout	ユーザ セッションが終了し、ユーザがログオフされます。

CLI を使用した初期設定

*注: この項で説明する、CLI を使用した手順の実行は任意です。KX III ローカル コンソールで同じ設定作業を実行できるからです。詳細については、「***最初に行う作業***』9p. の"***入門***"参照』」を参照してください。*

KX III は、デフォルト値に設定された状態で工場から出荷されます。初めて電源を入れて接続を行う際、次のとおりに基本パラメータ値を設定し、ネットワーク上から KX III に安全にアクセスできるようにする必要があります。

1. 管理者パスワードを再設定します。KX III は、すべてのデバイスに同じデフォルト パスワードが設定された状態で出荷されます。したがって、セキュリティ侵害を回避するため、管理者パスワードをデフォルトの raritan から変更する必要があります。新しいパスワードは、KX III の管理者になるユーザが決めます。
2. IP アドレス、サブネット マスク、およびデフォルト ゲートウェイの値を設定し、リモート アクセスできるようにします。

パラメータ値を設定する

パラメータ値を設定するには、管理者権限でログオンする必要があります。CLI 階層の最上位である username > プロンプトが表示されます。初期設定を行うため、admin と入力します。top コマンドを入力し、最上位レベルに戻ります。

注: admin 以外のユーザ名でログオンした場合、admin の代わりにそのユーザ名が表示されます。

ネットワーク パラメータの設定

ネットワーク パラメータ値を設定するには、interface コマンドを使用します。

```
admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode
auto
```

このコマンドが受け付けられると、KX III との接続が自動切断されます。新たに設定した IP アドレス、および、「パラメータ値を設定する」で作成したユーザ名とパスワードを使用して、KX III に再接続します。

重要: パスワードを忘れてしまった場合は、KX III の背面にあるリセット ボタンを押し、出荷時設定に戻す必要があります。この場合、初期設定作業を再度実行する必要があります。

これで KX III の基本情報が設定されたので、SSH またはグラフィカル ユーザ インタフェース (GUI) を使用してリモート アクセスすることや、ローカル シリアル ポートを使用してローカル アクセスすることができます。管理者は、ユーザ、グループ、サービス、セキュリティ、およびシリアル ポートを設定する必要があります。シリアル ポートは、シリアル ターゲットを KX III に接続するためのポートです。

CLI プロンプト

CLI プロンプトは、現在のコマンド レベルを意味しています。プロンプトのルート部分はログオン名です。端末エミュレーション ソフトウェアを使用して管理用シリアル ポートに直接接続している場合、コマンドのルート部分は Admin Port になります。

```
admin >
```

CLI コマンド

- `admin > help` と入力した場合に使用できるコマンドは、次のとおりです。

コマンド	説明
config	config サブメニューに切り替えます。
diagnostics	diag サブメニューに切り替えます。
help	コマンドの概要を表示します。
history	現在のセッションのコマンド ライン履歴を表示します。
listports	使用可能なポートを一覧表示します。
logout	現在の CLI セッションを終了し、ログオフします。
top	ルート メニューに戻ります。
userlist	アクティブなユーザ セッションを一覧表示します。

- 「admin > config > network」と入力します。

コマンド	説明
help	コマンドの概要を表示します。
history	現在のセッションのコマンド ライン履歴を表示します。
interface	ネットワーク パラメータ値を取得および設定します。
ipv6_interface	IPv6 のネットワーク パラメータ値を取得および設定します。
logout	現在の CLI セッションを終了し、ログオフします。
name	デバイス名を設定します。
quit	前のメニューに戻ります。
stop	ルート メニューに戻ります。

セキュリティ上の問題

コンソール サーバにおけるセキュリティを確保する際に検討すべき点は、次のとおりです。

- 運用担当者用コンソールと KX III との間で送受信されるデータ トラフィックを暗号化する。
- ユーザに対して認証を行い、また、ユーザに付与する権限を制限する。
- セキュリティ プロファイルを設定する。

KX III にはこの 3 つの機能がすべて備わっています。ただし、設定作業は運用開始前に済ませておく必要があります。

KX III コンソール サーバ設定用コマンドを使用する

注:SSH 接続とローカル ポート接続では、CLI コマンドは同じです。

network コマンドは、Configuration メニューで使用できます。

ネットワークを設定する

network メニューのコマンドを使用して、KX III のネットワーク インタフェースを設定します。

コマンド	説明
interface	KX III のネットワーク インタフェースを設定します。
name	ネットワーク名を設定します。
ipv6	IPv6 のネットワーク パラメータ値を取得および設定します。

interface コマンド

interface コマンドを使用して、KX III のネットワーク インタフェースを設定します。**interface コマンドの構文は次のとおりです。**

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask <subnetmask>] [gw <ipaddress>] [mode <mode>]

Ethernet パラメータ値を設定/取得します。

ipauto <none|dhcp>: IP アドレスを自動設定するかどうか (none/dhcp)。

ip <ipaddress>: IP アドレス。

mask <subnetmask>: サブネット マスク。

gw <ipaddress>: デフォルト ゲートウェイ。

mode <mode>: Ethernet モードを設定 (auto/10hdx/10fdx/100hdx/100fdx/1000fdx)。
```

interface コマンドの例

次のコマンドを実行すると、インタフェース番号 1 が有効になり、IP アドレス、サブネット マスク、およびデフォルト ゲートウェイの値が設定され、Ethernet モードが自動検出に設定されます。

```
Admin > Config > Network > interface ipauto none ip 192.16.151.12 mask 255.255.255.0 gw 192.168.51.12 mode auto
```

name コマンド

name コマンドを使用して、ネットワーク名を設定します。name コマンドの構文は次のとおりです。

```
name [devicename <devicename>] [hostname <hostname>]
```

デバイス名の設定

```
devicename <devicename>: デバイス名。
hostname <hostname>: 優先ホスト名 (DHCP 使用時のみ)。
```

name コマンドの例

次のコマンドを実行すると、ネットワーク名が設定されます。

```
Admin > Config > Network > name devicename My-KSX2
```

ipv6 コマンド

ipv6 コマンドを使用して、IPv6 関連のネットワーク パラメータ値の設定と取得を行います。

```
Ipv6_interface mode enable ipauto none ip
2001:db8:290c:1291::17 prefixlen 128 gw
2001:db8:290c:1291::1
```

デュアル ビデオ ポート グループ

ビデオ カードを 2 枚搭載したサーバには、拡張デスクトップ設定を利用してリモートからアクセスできます。この設定は、リモート ユーザが利用できます。このためには、デュアル ポート ビデオ グループを作成します。

拡張デスクトップ設定により、標準的な 1 台のモニタでの表示に対して 2 台のモニタでターゲット サーバのデスクトップを表示できるようになります。

デュアル ポート ビデオ グループを選択すると、そのグループのポート チャネルがすべて同時に開かれます。

「**デュアル ビデオ ポート グループの作成** 『166p. 』」 を参照してください。

デュアル ポート ビデオ グループに関する重要な情報については、このセクションの内容を確認してください。

注:デュアル ポート ビデオ グループは、KX3-108 や KX3-116 のような、KVM チャネルが 1 つしかないモデルではサポートされていません。

デュアル ポート ビデオに関する推奨事項

マウスの同期を維持して定期的な再同期を最小限に抑えるために、ターゲット サーバのプライマリ画面およびセカンダリ画面を同じ画面解像度に設定してください。

設定する方向に応じて、上の画面（垂直方向）または左の画面（水平方向）をプライマリ画面として指定する必要があります。この画面で、仮想メディア、音声、スマート カード、およびマウスを操作するためのアクティブなメニュー選択が可能になります。

直観的なマウスの動作や制御を実現するために、

- クライアント PC のプライマリ画面とセカンダリ画面
- KX II/KX III のデュアル ビデオ ポート グループ設定
- ターゲット サーバのプライマリ画面とセカンダリ画面

デュアル ポート ビデオ画面には、次のクライアント起動設定だけが適用されます。

- KVM クライアントを起動する場合は、標準画面または全画面ウィンドウ モードを選択する
- ビデオの拡大/縮小を有効にする
- 全画面モードのときにメニュー ツールバーの固定機能を有効にする

1 台のクライアント モニタでデュアル ビデオ ポートを全画面モードで表示する場合、シングル マウス モードの使用はお勧めできません。このような場合は、シングル マウス モードを終了してから、他方の画面にアクセスして表示する必要があります。

デュアル ビデオ ポート グループでサポートされているマウス モード

対象のオペレーティング システム	サポートされているマウス モード	コメント
すべての Windows® オペレーティング システム	インテリジェント モード、標準モード、およびシングル マウス モード	ターゲット サーバのビデオ カードで「ストレッチ」モードがサポートされている場合は、ずれないマウス モードが正しく動作します。 ストレッチ モードにより、ターゲット サーバでは、2 つの画面が 1 つの仮想画面として管理されます。 それに対して、拡張モードで設定されている場合、各画面は 2 つの独立した画面と見なされます。拡張モードの場合は、イ

対象のオペレーティング システム	サポートされているマウス モード	コメント
		ンテリジェント マウス モードにすることをお勧めします。
Linux®	インテリジェント マウス モードおよび標準マウス モード	Linux® ユーザは、シングル マウス モードを使用すると画面やマウスの動作に関する問題が発生する場合があります。Linux ユーザは、できればシングル マウス モードを使用しないでください。
Mac® オペレーティング システム	シングル マウス モード	複数のモニタを備えた Mac ターゲットの場合は、標準マウスをシングル カーソル モードで使用します。

デュアル ビデオ サポートに必要な CIM

以下の CIM は、デュアル ビデオ ポート機能をサポートしています。

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-DP
- D2CIM-DVUSB-HDMI
- DCIM-USBG2

デジタル CIM に関する重要な情報については、「デジタル CIM ターゲット サーバのタイミングおよび画面解像度」を確認してください。CIM の仕様については、「サポートされているコンピュータ インタフェース モジュール (CIM) の仕様」を参照してください。

プライマリまたはセカンダリ ビデオ ポートに接続されている元の DCIM が切断され、別の CIM に切り替えられると、そのポートはデュアル ポート ビデオ グループから削除されます。必要に応じて、ポートをグループに追加し直します。

注:使用する CIM は、ターゲット サーバの要件によって異なります。

デュアル ポート ビデオ グループの使いやすさに関する注意事項

以下は、デュアル ポート ビデオ グループ機能を使用するときに影響を受ける各種機能です。

- [Tools] (ツール) メニューの [Options] (オプション) の [Client Launch Settings] (クライアント起動設定) を介して Virtual KVM Client (VKC) および Active KVM Client (AKC) のクライアントで設定されるクライアント起動設定は、次のようにデュアル ビデオ ポート グループに適用されます。
  - ウィンドウ モード設定が適用されます。
  - モニタ設定は適用されません。代わりに、[Port Group Management] (ポート グループ管理) で設定した「画面の方向」が適用されます。
  - その他 - [Enable Single Mouse Cursor] (シングル マウス カーソルを有効にする) 設定は適用されません。
  - その他 - [Enable Scale Video] (ビデオの拡大、縮小を有効にする) 設定が適用されます。
  - その他 - [Pin Menu Toolbar] (メニュー ツールバーを常に表示) 設定が適用されます。
- プライマリ ターゲットとセカンダリ ターゲットのウィンドウ間で項目をドラッグして移動する場合は、マウス ボタンを押したまま移動して離すと、一方のウィンドウから他方のウィンドウに項目が移動されます。
- Linux® および Mac® のターゲット サーバで、Caps Lock および Num Lock をオンにすると、プライマリ ポート ウィンドウのステータス バーに Caps Lock インジケータが表示されますが、このインジケータは、セカンダリ ポート ウィンドウのステータス バーには表示されないことがあります。

権限およびデュアル ビデオ ポート グループ アクセス

理想的には、ポート グループの各ポートに適用される権限は、同じでなければなりません。権限が同じでない場合は、最も制限の厳しいポートの権限がポート グループに適用されます。

たとえば、あるポートに [VM Access] (VM アクセス) の [Deny] (拒否) が適用されており、別のポートに [VM Access] (VM アクセス) の [Read-Write] (読み取り/書き込み可能) が適用されている場合、ポート グループには、[VM Access] (VM アクセス) の [Deny] (拒否) が適用されます。

デュアル ポート ビデオ グループに属しているポートにアクセスするための適切な権限がないユーザには、アクセスできるポートだけが表示されます。どのポートにアクセスする権限もない場合、アクセスは拒否されます。

それでもポートにアクセスしようとすると、ポートを利用できないか、ポートにアクセスするための権限がないことを示すメッセージが表示されます。

デュアル ポート ビデオ グループ設定の例

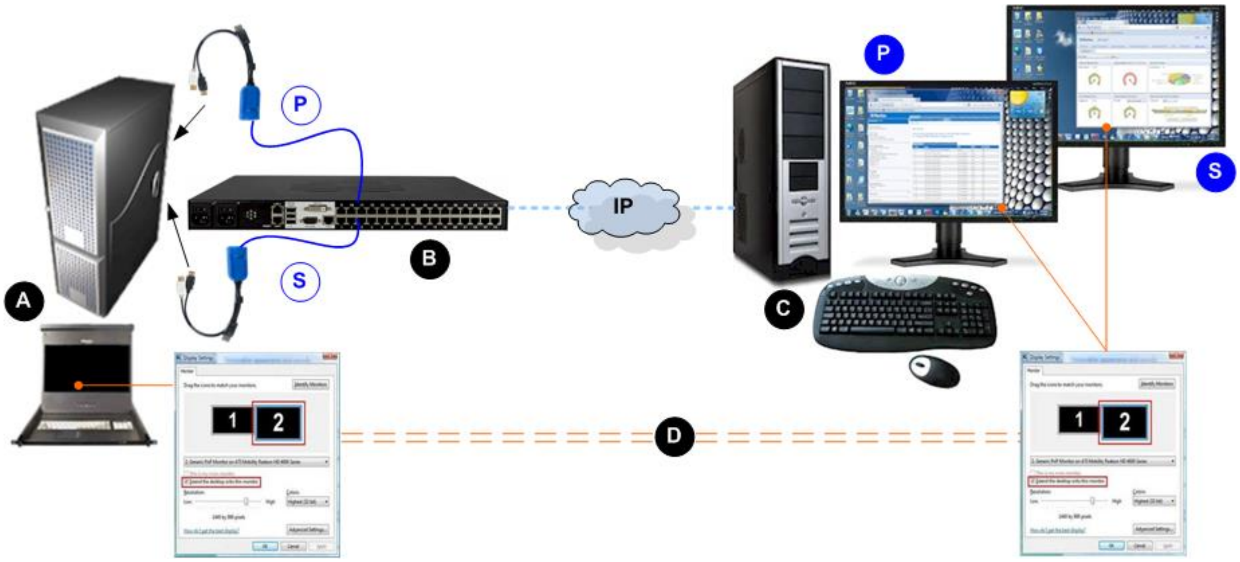
以下に、一般的な例を示します。

設定は、使用する CIM のタイプ、プライマリ ポートとして指定するポート、接続先のポートなどによって変わる可能性があります。

この例では、以下を前提にしています。

- 2 つのビデオ ポートを搭載したターゲット サーバ
- ターゲット サーバのビデオ ポート 1 がプライマリ ポート、およびビデオ ポート 2 がセカンダリ ポート
- KX3-832 デバイス
- D2CIM-DVUSB-DP CIM
- Microsoft® Windows 7® オペレーティング システムが稼動しているターゲット サーバおよびリモート クライアント
- インテリジェント マウス モード

ターゲット サーバおよびリモート クライアントで拡張デスクトップを表示するので、画面の方向が「水平 - プライマリ (左)、セカンダリ (右)」になるように KX III を設定しています。



図の説明	
A	リモート クライアント - デュアル ビデオ ポート グループおよび画面の設定
B	KX III

図の説明	
P	ターゲットのプライマリ（最初の）ビデオ ポートから KX III への接続
S	ターゲットのセカンダリ（2 番目の）ビデオ ポートから KX III への接続
KX III とリモート クライアント間の IP 接続	
C	ターゲット サーバ - 画面の設定およびデュアル ビデオ ポート グループの起動
D	画面の設定はリモート クライアントとターゲット サーバで同じ（推奨）
P	水平 - プライマリ（左）- KX III の [Port Group Management]（ポート グループ管理）ページで定義済み
S	セカンダリ（右）- KX III の [Port Group Management]（ポート グループ管理）ページで定義済み

デュアル ビデオ ポート設定手順

手順 1: ターゲット サーバの画面の設定

デバイスで設定されている、ターゲットの方向設定が、ターゲットのオペレーティング システムでの実際の設定と一致している必要があります。

できる限り、接続元のクライアントの画面方向を同じに設定しておくことをお勧めします。

画面の方向およびマウス モードについては、「デュアル ビデオ ポート グループの画面の方向、位置合わせ、およびマウス モード」 を確認してください。

注:画面の設定の指定方法に関する正確な手順については、ターゲット サーバまたはオペレーティング システムのユーザ マニュアルを参照してください。

▶ **ターゲット サーバの画面の設定およびマウスの設定を指定するには、以下の手順に従います。**

1. ターゲット サーバで、ビデオ ポートごとにターゲット サーバの画面の方向を、リモート クライアントの画面の方向と一致するように設定します。

たとえば、リモート クライアントで 2 つのモニタにわたって左から右に移動するように拡張デスクトップの方向を設定している場合は、ターゲット サーバの画面の方向を同じに設定します。

2. ターゲット サーバのビデオが、サポートされている解像度とリフレッシュ レートに設定されていることを確認します。***サポートされているターゲット サーバ画面解像度*** 『*336*p. の"*KX III でサポートされているターゲット サーバ画面解像度*"参照，*http://www.raritan.com/help/kx-iii/v3.0.0/en/index.htm#32872*』」 を参照してください。

注: ターゲットのプライマリ画面とセカンダリ画面の解像度の設定が異なっている場合は、マウスの同期が維持されなくなるので、左上のターゲット ウィンドウで定期的に再同期する必要があります。

手順 2: KX III へのターゲット サーバの接続

デュアル ポート ビデオ グループは、既存のポート接続または新しいポート接続から作成できます。

ここに示す手順では、新しい接続を作成すると想定しています。

既存の接続からデュアル ポート ビデオ グループを作成する場合は、「手順 4: デュアル ビデオ ポート グループの作成」を参照してください。

▶ 機器を接続するには、以下の手順に従います。

1. まだの場合は、製造元の手順に従ってターゲット サーバを設置し、電源を投入します。
2. 各 CIM のビデオ コネクタをターゲットの各ビデオ出力ポートに接続し、USB ケーブルをターゲット上の使用可能な USB ポートに接続します。
3. CAT5/6 ケーブルを使用して各 CIM を KX III に接続します。
4. 接続がまだの場合は、以下の手順に従います。
    a. 用意されている電源ケーブルを使用して KX III を AC 電源に接続します。
    b. KX III のネットワーク ポートおよびローカル ポート（必要な場合）に接続します。
    c. KX III を設定します。デバイスの使用を開始するために必要な手順については、「***入門*** 『*9*p. 』」を参照してください。
5. サポートされている Web ブラウザを起動します。
6. 次のどちらかを入力します。
    - URL: *http://IP-ADDRESS*（Java ベースの Virtual KVM Client を使用する場合）

      または

- *http://IP-ADDRESS/akc* (Microsoft .NET ベースの Active KVM Client の場合)

IP-ADDRESS は、KX III に割り当てられた IP アドレスです。

また、HTTPS を使用するか、管理者によって割り当てられた、KX III の DNS 名 (適用可能な場合) を使用することもできます。

常に、HTTP の IP アドレスから HTTPS の IP アドレスにリダイレクトされます。

7. ユーザ名とパスワードを入力して、[Login] (ログイン) をクリックします。
8. ユーザ同意書に承諾します (該当する場合)。
9. セキュリティ警告が表示される場合は、アクセスの承諾または許可、あるいはその両方を行います。

手順 3: マウス モードおよびポートの設定

ターゲット サーバのビデオ ポートを介してターゲット サーバを KX III に接続すると、その接続が検出され、[Port Configuration] (ポート設定) ページに該当するポートが表示されます。

手順については、「**標準ターゲット サーバの設定**」 を参照してください。

ポートを設定した後に、それらのポートをデュアル ビデオ ポート グループにまとめることができます。

---

*注:デュアル ビデオ ポート グループの作成時に、既存のポートが既に設定されている場合は、そのポートを設定する必要はありません。「**デュアル ビデオ ポート グループの作成**『166p. 』」 を参照してください。*

ターゲットに接続した後にターゲット サーバのマウス モードを設定します。「**デュアル ビデオ ポート グループでサポートされているマウス モード** 『224p. 』」 を参照してください。

手順 4: デュアル ビデオ ポート グループの作成

「***デュアル ビデオ ポート グループの作成*** 『*166*p. 』」を参照してください。

手順 5: デュアル ビデオ ポート グループを開く

デュアル ビデオ ポート グループを作成したら、そのグループを [Port Access] (ポート アクセス) ページで使用できます。

プライマリ ポートのクリックによってデュアル ビデオ ポート グループにリモート接続するには、2 つの KVM チャネルが必要です。2 つのチャネルを利用できない場合、接続リンクは表示されません。

KX III で設定されているセッション タイムアウトは、デュアル ビデオ グループの両方のポートに適用されます。

▶ デュアル ポート ビデオ グループを開くには、以下の手順に従います。

- [Port Access] (ポート アクセス) ページで、プライマリ ポート名をクリックし、[Connect] (接続) をクリックします。

一度に両方の接続が開かれ、2 種類のウィンドウに表示されます。

ウィンドウが表示されたら、使用している画面の設定に基づいてウィンドウを移動できます。たとえば、拡張デスクトップ モードを使用している場合は、ポート ウィンドウをモニタ間で移動できます。

デュアル ビデオ ポート グループを使用する際の Raritan クライアントの画面操作

クライアントで全画面モードを使用する場合は、次の方法でポートを切り替えます。

- VKC
  - Alt+Tab キーを押す
  - Mac® クライアントの場合は、F3 キーを押して、ポート画面を選択する
- AKC
  - 表示ウィンドウの外でマウスをクリックし、Alt+Tab キーを押す

ダイレクト ポート アクセスおよびデュアル ポート ビデオ グループ

ダイレクト ポート アクセス機能を利用した場合、ユーザはデバイスの [Login] (ログイン) ダイアログ ボックスと [Port Access] (ポート アクセス) ページを使用する必要がなくなります。

この機能を使用すると、ユーザ名とパスワードが URL に含まれていない場合に、ユーザ名とパスワードを直接入力してターゲットにアクセスすることもできます。

デュアル ポート ビデオ グループに属しているターゲットにアクセスする場合は、ダイレクト ポート アクセスにより、プライマリポートを使用して、プライマリ ポートおよびセカンダリ ポートの両方を開きます。

セカンダリ ポートへのダイレクト ポート接続は拒否され、通常の権限ルールが適用されます。

デュアル ポート ビデオ グループ機能については、「**デュアル ビデオ ポート グループの作成** 『166p. 』」を参照してください。.

ダイレクト ポート アクセスについては、「**URL を経由したダイレクト ポート アクセスの有効化**」を参照してください。

[Ports] (ポート) ページに表示されるデュアル ポート ビデオ グループ

注: デュアル ビデオ プライマリ ポートは、ポート グループの作成時に定義されます。

注: プライマリ ポートのクリックによってデュアル ビデオ ポート グループにリモート接続するには、2 つの KVM チャネルが必要です。2 つのチャネルを利用できない場合、接続リンクは表示されません。

デュアル ビデオ ポート グループでは、プライマリ ポートはポート スキャンの対象になりますが、リモート クライアントから接続する場合、セカンダリ ポートは対象になりません。両方のポートをローカル ポートからスキャンの対象にすることができます。

[Ports] (ポート) ページに表示される内容の詳細については、「[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)」を参照し、スキャンの実行については、「ポートのスキャン」を参照してください。

LDAP スキーマを更新する

ユーザ グループ情報を返す

この章で説明する内容に従って、ユーザ認証の成功後にユーザ グループ情報を返すように設定してください。ユーザ グループ情報は、ユーザへの権限付与に役立ちます。

LDAP/LDAPS から返す場合

LDAP/LDAPS 認証に成功すると、KX III では、そのユーザの所属グループに付与されている権限に基づいて、そのユーザに付与する権限が決まります。リモート LDAP サーバから次のような属性が返されるので、ユーザ グループ名がわかります。

rciusergroup　　attribute type: string

このように属性を返すには、LDAP/LDAPS サーバ上でスキーマを拡張しなければばならないことがあります。認証サーバ管理者に連絡し、この属性を有効にしてください。

また、Microsoft® Active Directory® の場合、標準 LDAP memberOf が使用されます。

Microsoft Active Directory から返す場合

注:この手順は、経験豊富な Active Directory® 管理者だけが行ってください。

Windows 2000® オペレーティング システム サーバ 上の Microsoft® Active Directory からユーザ グループ情報を返すには、LDAP/LDAPS スキーマを更新する必要があります。詳細については、Microsoft 発行のドキュメントを参照してください。

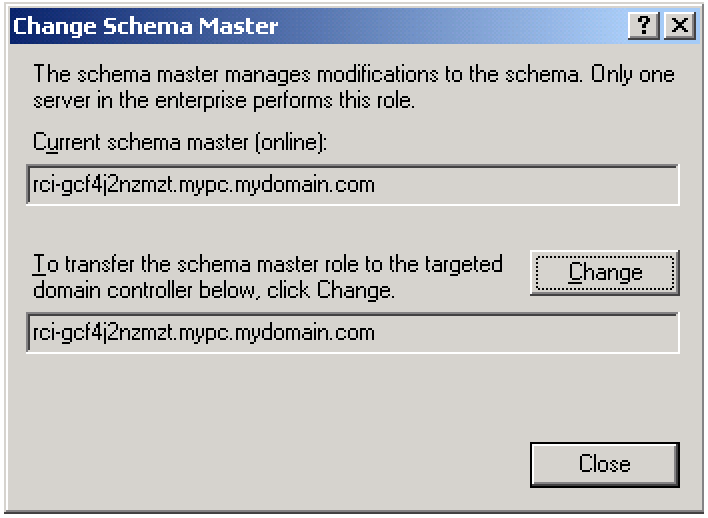
1. Active Directory 用のスキーマ プラグインをインストールします。インストール手順については、Active Directory のドキュメントを参照してください。
2. Active Directory コンソールを起動し、[Active Directory Schema] (Active Directory スキーマ) を選択します。

スキーマへの書き込み操作を許可するようにレジストリを設定する

ドメイン コントローラによるスキーマへの書き込みを許可するため、スキーマの更新を許可するレジストリ エントリを設定する必要があります。

▶ スキーマへの書き込みを許可するには

1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) ルート ノードを右クリックし、コンテキスト メニューの [Operations Master] (操作マスタ) をクリックします。[Change Schema Master] (スキーマ マスタの変更) ダイアログ ボックスが開きます。



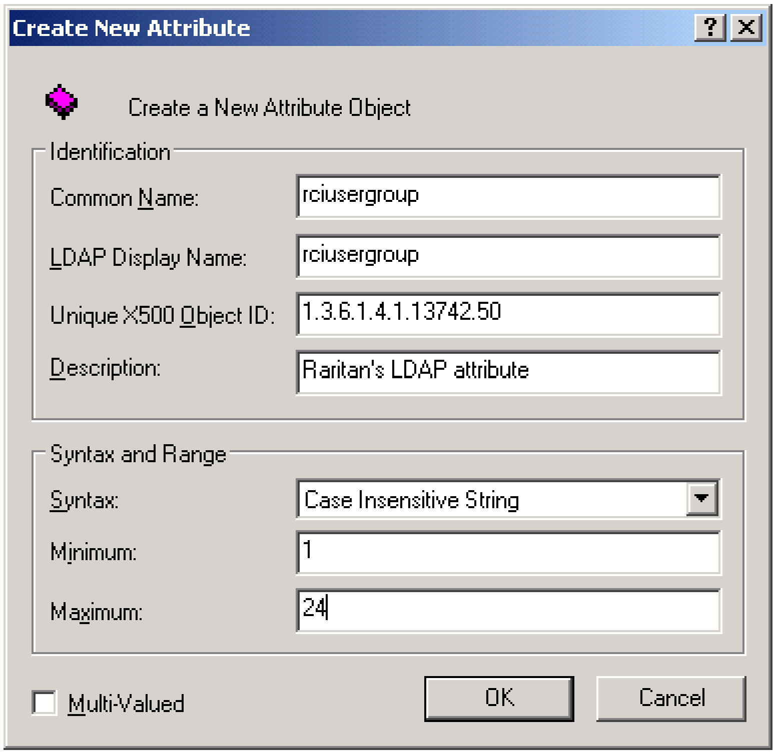
2. [Schema can be modified on this Domain Controller] (このドメイン コントローラでスキーマを修正できるようにする) チェック ボックスをオンにします。**(オプション)**
3. [OK] をクリックします。

新しい属性を作成する

▶ rciusergroup クラスに対する新しい属性を作成するには

1. ウィンドウの左ペインで、[Active Directory Schema] (Active Directory® スキーマ) の前に表示されている [+] (+) 記号をクリックします。
2. 左ペインで [Attributes] (属性) を右クリックします。

3. コンテキスト メニューの [New] (新規) をクリックし、続いて [Attribute] (属性) をクリックします。警告メッセージが表示されたら、[Continue] (続行) をクリックします。[Create New Attribute] (属性の新規作成) ダイアログ ボックスが開きます。



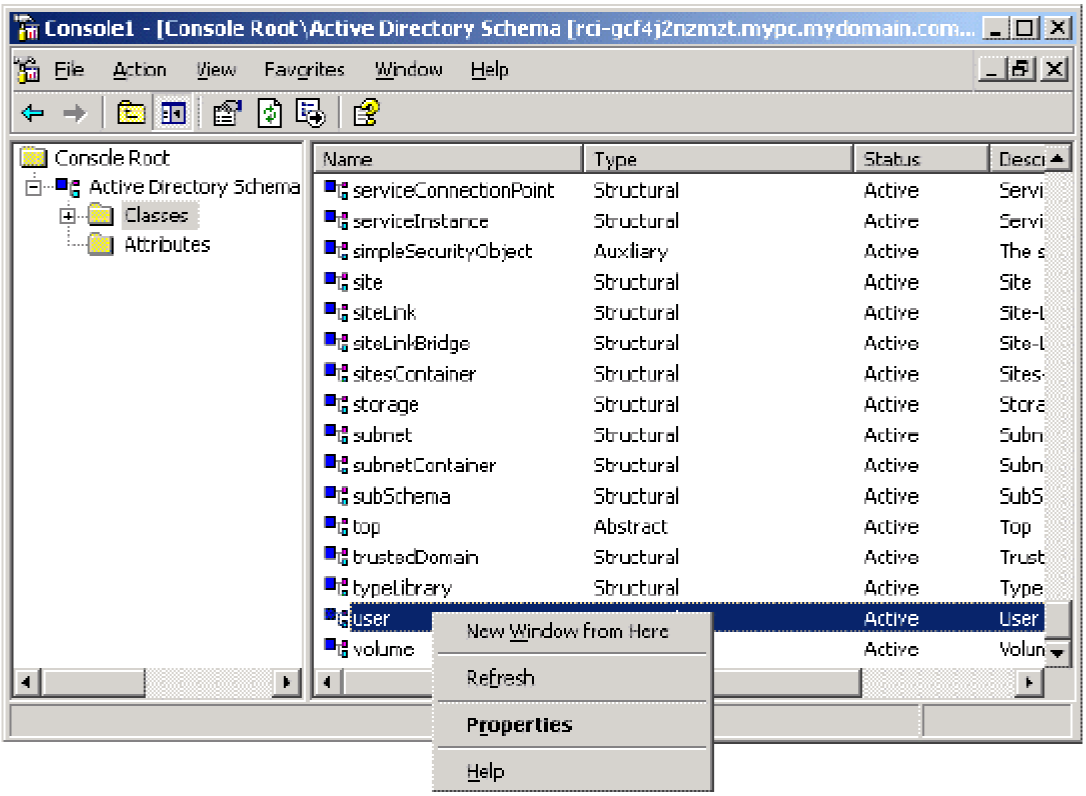
4. [Common Name] (共通名) ボックスに「rciusergroup」と入力します。
5. [LDAP Display Name] (LDAP 表示名) ボックスに「rciusergroup」と入力します。
6. [Unique X500 Object ID] (一意の X.500 オブジェクト ID) フィールドに「1.3.6.1.4.1.13742.50」と入力します。
7. [Description] (説明) ボックスにわかりやすい説明を入力します。
8. [Syntax] (構文) ボックスの一覧で [Case Insensitive String] (大文字/小文字の区別がない文字列) を選択します。
9. [Minimum] (最小) ボックスに「1」と入力します。
10. [Maximum] (最大) ボックスに「24」と入力します。
11. [OK] をクリックし、新しい属性を作成します。

属性をクラスに追加する

▶ 属性をクラスに追加するには

1. ウィンドウの左ペインで [Classes] (クラス) をクリックします。

2. 右ペインをスクロールして [user] (user) を表示し､右クリックします。



3. コンテキスト メニューの [Properties] (プロパティ) をクリックします。[user Properties] (user のプロパティ) ダイアログ ボックスが開きます。
4. [Attributes] (属性) タブをクリックしてそのプロパティ ページを開きます。
5. [Add] (追加) をクリックします。

6. [Select a schema object] (スキーマ オブジェクトを選択) ボックスの一覧で [rciusergroup] (rciusergroup) を選択します。

7. [Select Schema Object] (スキーマ オブジェクトを選択) ダイアログ ボックスで [OK] をクリックします。
8. [user Properties] (user のプロパティ) ダイアログ ボックスで [OK] をクリックします。

スキーマ キャッシュを更新する

▶ スキーマ キャッシュを更新するには

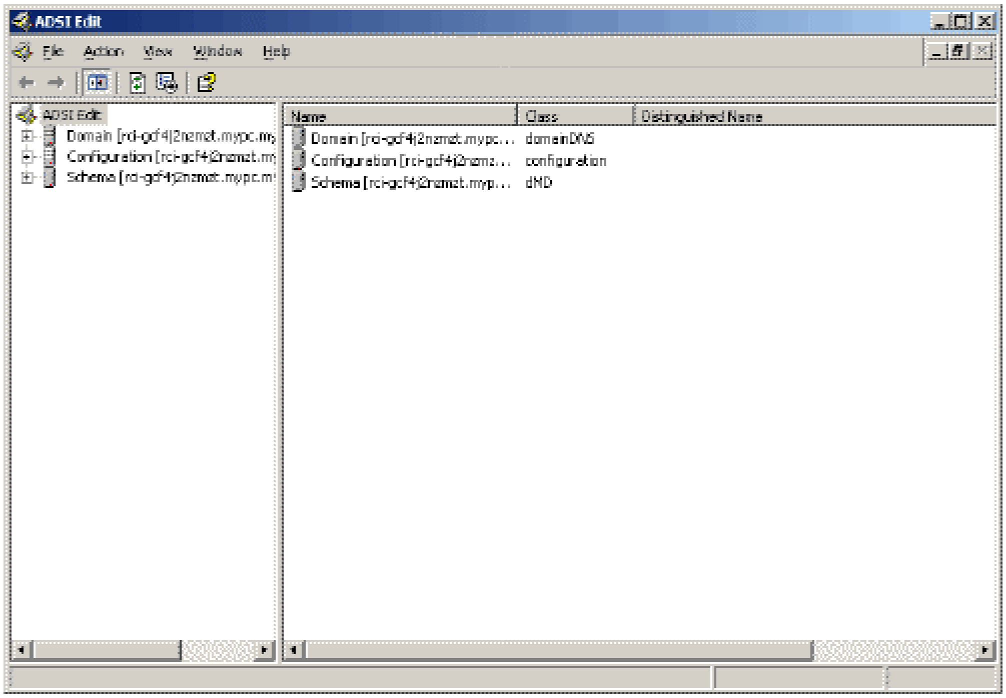
1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) を右クリックし、コンテキスト メニューの [Reload the Schema] (スキーマを再ロード) を選択します。
2. Active Directory スキーマ MMC コンソール (Microsoft® Management Console) を最小化します。

ユーザ メンバの rciusergroup 属性を編集する

Windows Server 2003® 上で Active Directory® スクリプトを実行するには、Microsoft® から提供されるスクリプトを使用します (Windows Server 2003 のインストール用 CD-ROM に収録されています)。これらのスクリプトは、Microsoft® Windows 2003 のインストール時にシステムにロードされます。Active Directory Service Interface (ADSI) は、Active Directory の下位レベルのエディタとして動作します。これにより、オブジェクトの追加、削除、移動などの一般的な管理作業を、ディレクトリ サービスを使用して行うことができます。

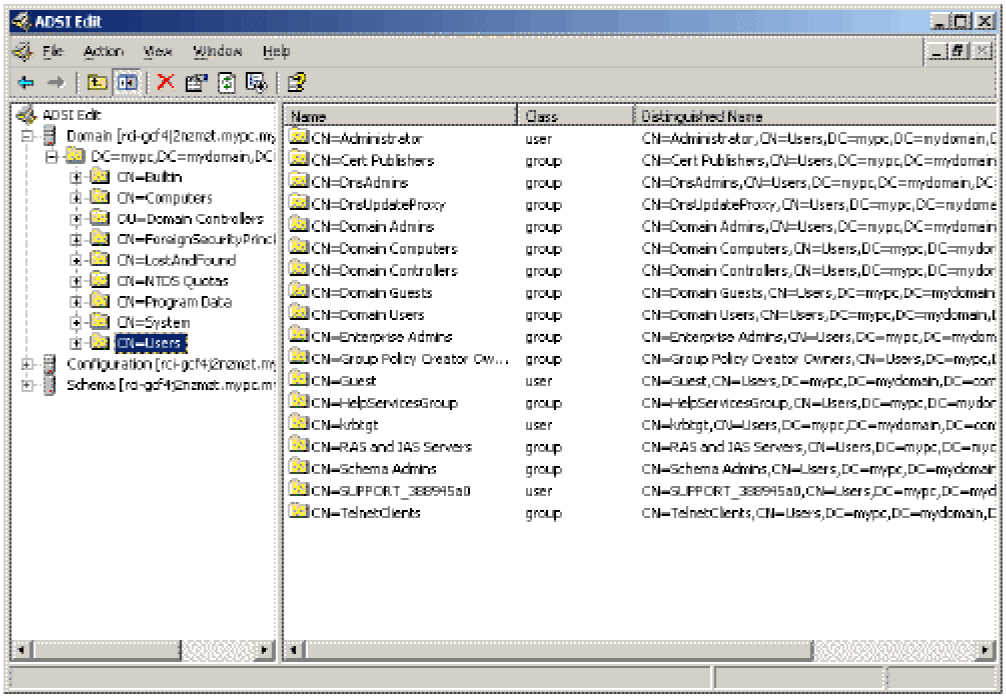
▶ rciusergroup グループ内の個別のユーザ属性を編集するには、以下の手順に従います。

1. Windows Server 2003 のインストール用 CD-ROM を挿入し、エクスプローラで Support フォルダの下の Tools フォルダを開きます。
2. SUPTOOLS.MSI をダブルクリックし、サポート ツールをインストールします。
3. サポート ツールがインストールされたフォルダを開きます。adsiedit.msc を実行します。[ADSI Edit] (ADSI 編集) ウィンドウが開きます。



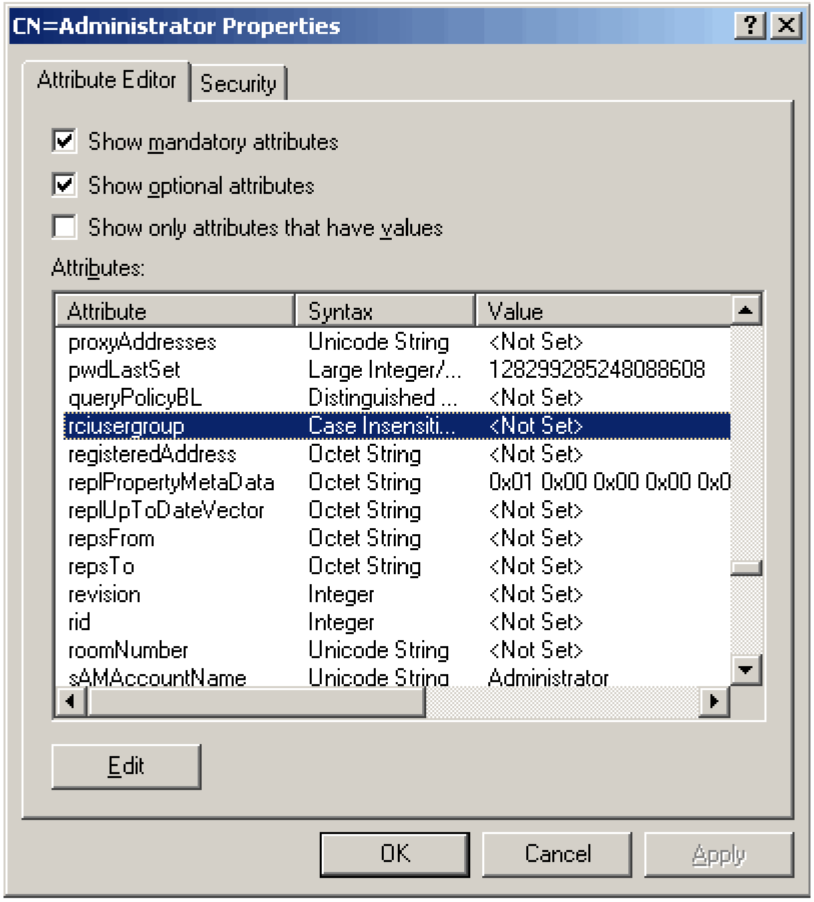
4. [Domain] (ドメイン) を開きます。

5. ウィンドウの左ペインで CN=Users フォルダを選択します。



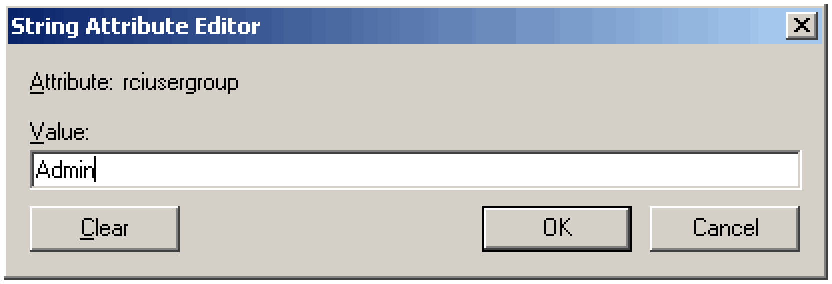
6. 右ペインで、プロパティ値を編集したいユーザ名を探します。ユーザ名を右クリックし、コンテキスト メニューの [Properties] (プロパティ) をクリックします。

7. [Attribute Editor] (属性エディタ) タブをクリックします。[Attributes] (属性) ボックスの一覧で [rciusergroup] (rciusergroup) を選択します。



8. [Edit] (編集) をクリックします。[String Attribute Editor] (文字列属性エディタ) ダイアログ ボックスが開きます。

9. [Value] (値) ボックスに、KX III で作成したユーザ グループを入力します。[OK] をクリックします。



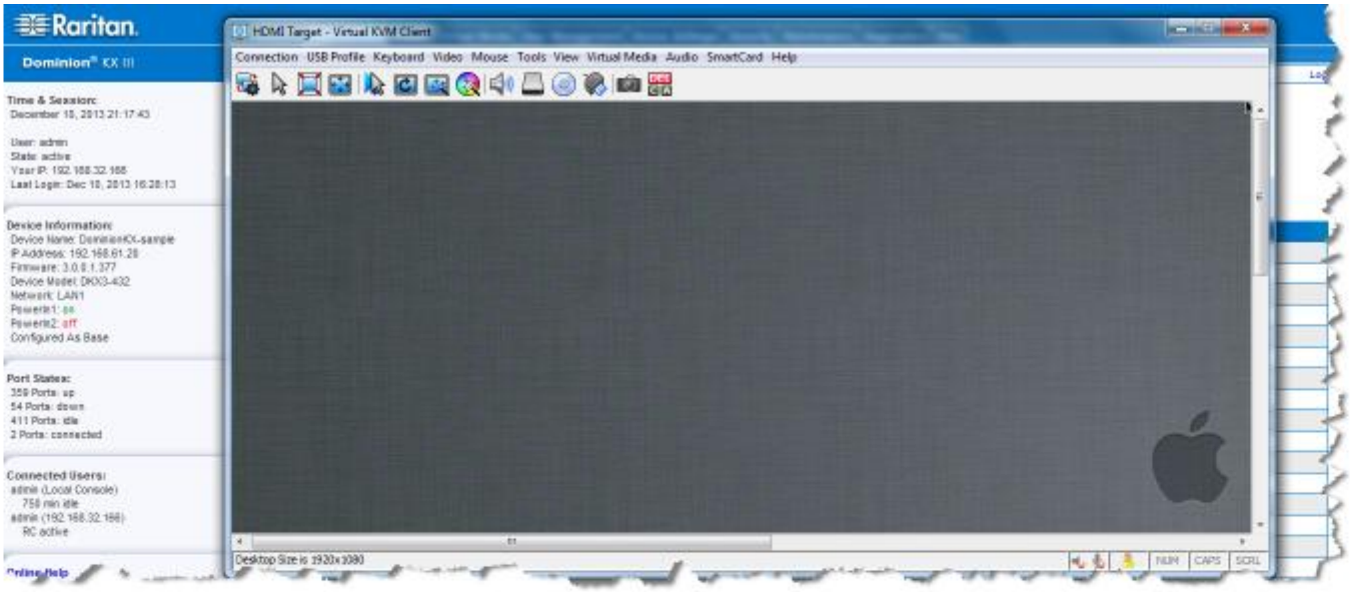
Ch 5 Virtual KVM Client (VKC) ヘルプ

この章の内容

概要 242
ターゲット サーバへの接続 243
接続プロパティの設定 244
接続情報 248
USB プロファイル 249
キーボード 250
ビデオのプロパティ 255
マウス オプション 259
ツール オプション 263
表示オプション 270
仮想メディア 272
スマート カード 281
デジタル音声 284
バージョン情報 － Virtual KVM Client 292

概要

KX III リモート コンソールの [Port Access] (ポート アクセス) ページからターゲット サーバにアクセスすると、必ず Virtual KVM Client (VKC) のウィンドウが開かれます。



接続されているターゲット サーバごとに 1 つの Virtual KVM Client ウィンドウが表示されます。

Virtual KVM Client ウィンドウは、お使いのコンピュータのデスクトップ上で最小化、最大化、および移動できます。

重要: ブラウザ表示を更新すると Virtual KVM Client 接続が切断されてしまうので注意してください。

Virtual KVM Client (VKC) および Active KVM Client (AKC) は、リモート ターゲットへのアクセスに使用されるインタフェースです。

VKC および AKC は、特徴が似ています。ただし、以下の点は除きます。

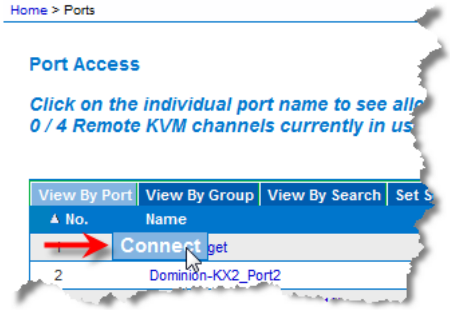
- 最小システム要件
- サポートされているオペレーティング システムとブラウザ
- AKC で作成されたキーボード マクロは、VKC では使用不可
- ダイレクト ポート アクセス設定 (「**URL を経由したダイレクト ポート アクセスの有効化**」を参照)
- AKC サーバ証明書検証設定 (「**AKC を使用するための前提条件**『296p. の"AKC を使用するため前提条件"参照 』」を参照)

ターゲット サーバへの接続

KX III リモート コンソールにログインしたら、Virtual KVM Client (VKC) または Active KVM Client (AKC) 経由でターゲット サーバにアクセスします。

利用可能なターゲット サーバまたはデュアル モニタ ターゲット サーバに接続するには、以下の手順に従います。

1. [Port Access] (ポート アクセス) ページで、接続するターゲット サーバのポート名をクリックします。[Port Action] (ポート アクション) メニューが開きます。
2. [接続] をクリックします。



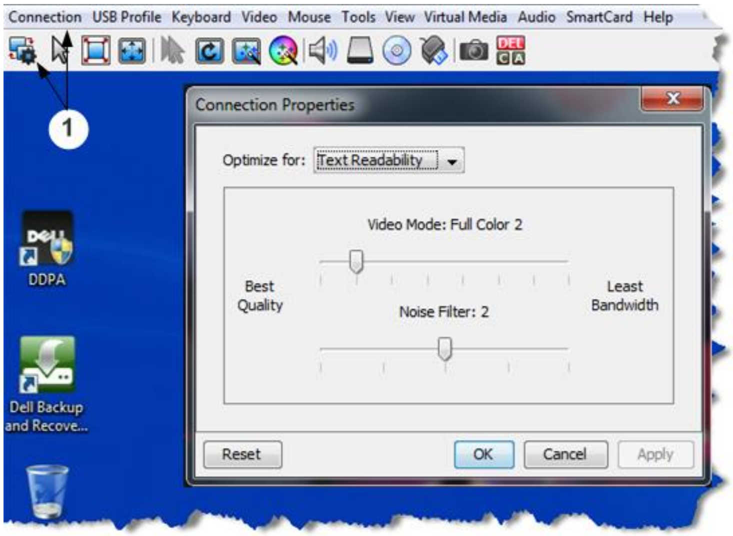
使用可能な他のメニュー オプションの詳細については、「*[Port Action] (ポート アクション) メニュー* 『*20*p. 』」を参照してください。

接続プロパティの設定

接続プロパティへのアクセス

▶ 接続プロパティにアクセスするには、以下の手順に従います。

1	[Connection] (接続) の [Properties] (プロパティ) をクリックするか、[Connection...] (接続...) アイコンをクリックして、[Connection Properties] (接続プロパティ) ダイアログ ボックスを開きます。



接続プロパティの概要

Virtual KVM Client (VKC) および Active KVM Client (AKC) では、接続プロパティの管理がサポートされています。

接続プロパティで、ターゲット サーバへのリモート接続経由のストリーミング ビデオ パフォーマンスを管理できます。

このプロパティは、自分が使用している接続にのみ適用され、VKC または AKC を介して同じターゲット サーバにアクセスしている他のユーザの接続には適用されません。

接続プロパティに変更を加えた場合、その変更は、VKC および AKC で保持されます。

デフォルトの接続プロパティ設定 - 最適化による最高のパフォーマンスの実現

KX III は、ほとんどのビデオ ストリーミング条件で最適なパフォーマンスが得られるように設定されています。

デフォルトの接続設定は、次のようになっています。

- [Optimize for] (最適化): [Text Readability] (テキストの読みやすさ) - ビデオ モードは、テキストの読みやすさが最大になります。

  この設定は、サーバ管理の実行などの一般的な IT アプリケーションやコンピュータ アプリケーションに最適です。

- [Video Mode] (ビデオ モード) - デフォルトでは [Full Color 2] (フルカラー 2) に設定されます。

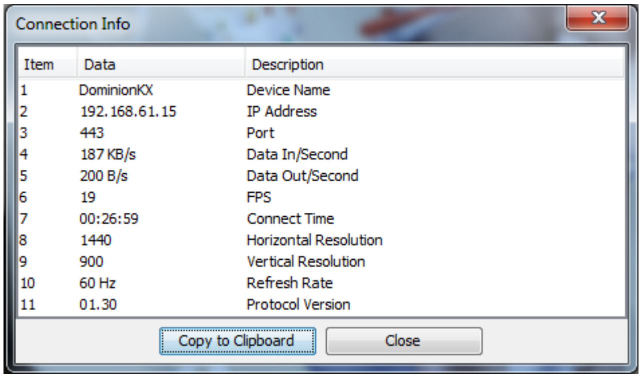
  ビデオ フレームは、高画質の 24 ビット カラーで送信されます。この設定は、高速 LAN を利用する場合に適しています。

- [Noise Filter] (ノイズ フィルタ) - デフォルトでは 2 に設定されます。

  通常は、ノイズ フィルタ設定を変更する必要はありません。

いつでも [Connection Properties] (接続プロパティ) ダイアログ ボックスで [Reset] (リセット) をクリックしてデフォルトの設定に戻します。

ヒント: [Connection Information] (接続情報) ダイアログ ボックスを使用して、接続をリアルタイムに監視します。 「**接続情報のアクセスおよびコピー** 『249p. 』」*を参照してください。*



[Optimize for] (最適化): 選択

[Text Readability] (テキストの読みやすさ)

[Text Readability] (テキストの読みやすさ) を選択すると、すべてのビデオ モードは、高画質になり、テキストが読みやすくなります。

この設定は、サーバ管理を実行するときなど、コンピュータの GUI を操作する場合に最適です。

フル カラー ビデオ モードで作業する場合は、コントラストがわずかに高められ、テキストがより鮮明になります。

低画質ビデオ モードでは、帯域幅が減少し、精度が低下します。

[Color Accuracy] (色精度)

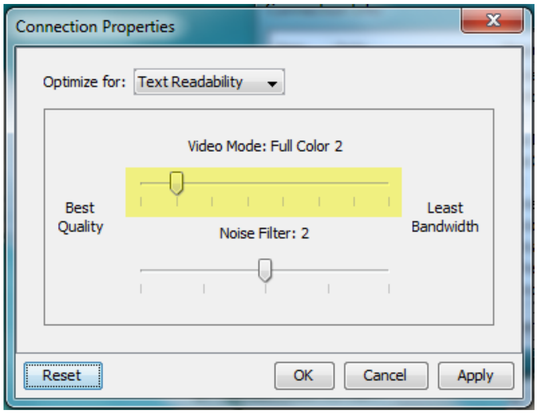
[Color Accuracy] (色精度)が選択されている場合、すべてのビデオ モードは、均一な色応答のフル カラーで表示されます。

この設定は、動画などのビデオ ストリームやその他のブロードキャスト ストリームの表示に適用されます。

低画質ビデオ モードでは、テキストなどの細部の鮮明さが低下します。

[Video Mode] (ビデオ モード)

[Video Mode] (ビデオ モード) スライダで、ビデオ品質、フレーム レート、および帯域幅に作用する、各ビデオ フレームのエンコードを制御します。



一般に、このスライダを左に動かすと、高画質となりますが、帯域幅は減少し、場合によっては、フレーム レートが低下します。

このスライダを右に動かすと、より強力に圧縮され、フレームあたりの帯域幅は減少しますが、ビデオ品質が低下します。

システム帯域幅が制限要因となっている場合には、ビデオ モード スライダを右に動かすと、フレーム レートが高くなる可能性があります。

最適化の設定として [Text Readability] (テキストの読みやすさ) が選択されている場合、右の 4 つのモードでは、色解像度が低下するか、色がなくなります。

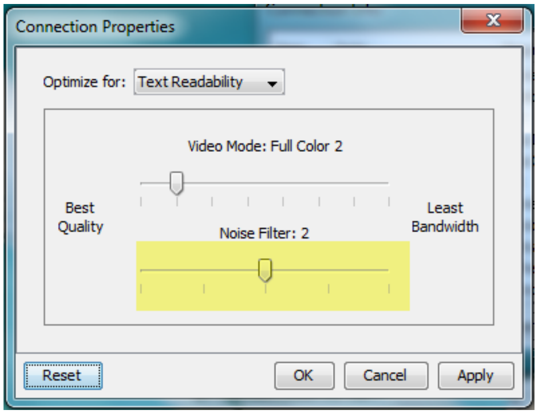
これらのモードは、テキストや GUI 要素が優先され、帯域幅が重要となる管理作業に適しています。

いつでも [Connection Properties] (接続プロパティ) ダイアログ ボックスで [Reset] (リセット) をクリックしてデフォルトの設定に戻します。

[Noise Filter] (ノイズ フィルタ)

特に必要がない限り、ノイズ フィルタ設定は変更しないでください。デフォルトの設定は、ほとんどの状況で十分に機能するようになっています。

[Noise Filter] (ノイズ フィルタ) では、フレーム間のノイズを KX III でどの程度吸収するかを制御します。



[Noise Filter] (ノイズ フィルタ) スライダを左に動かすと、フィルタしきい値が低くなり、よりダイナミックなビデオ品質となります。ただし、ノイズが増える可能性があるため、帯域幅が増大し、フレーム レートは低下します。

このスライダを右に動かすと、しきい値が高くなるため、ノイズが少なくなり、使用帯域幅は減少します。ビデオ アーチファクトは増える可能性があります。

ノイズ フィルタのスライダを右に動かすと、帯域幅が厳しく制限された接続でコンピュータ GUI にアクセスする場合に役立つ可能性があります。

いつでも [Connection Properties] (接続プロパティ) ダイアログ ボックスで [Reset] (リセット) をクリックしてデフォルトの設定に戻します。

接続情報

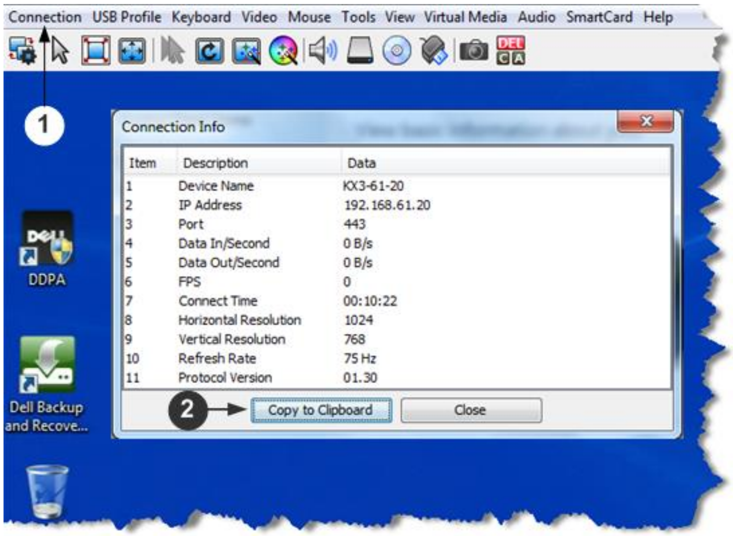
リアルタイム接続情報を表示する [Connection Information] (接続情報)ダイアログ ボックスを開き、必要に応じてダイアログ ボックスから情報をコピーします。

この機能が役に立つのは、現在の接続に関する情報をリアルタイムに収集したい場合などです。「*接続プロパティの設定* 『*244*p. 』」を参照してください。

現在の接続に関する以下の情報が表示されます。

- [KX III Name] (KX III 名) – KX III の名前です。
- [IP Address] (IP アドレス) – KX III の IP アドレスです。
- [Port] (ポート) – KX III へのアクセスに使用される KVM 通信 TCP/IP ポートです。
- [Data In/Second] (データ入力/秒) – KX III から受信したデータレートです。
- [Data Out/Second] (データ出力/秒) – KX III に送信したデータレートです。
- [Connect Time] (接続時間) – 現在の接続時間です。
- [FPS] – KX III と送受信したビデオ フレーム/秒です。
- [Horizontal Resolution] (水平解像度) – ターゲット サーバの水平解像度です。
- [Vertical Resolution] (垂直解像度) – ターゲット サーバの垂直解像度です。
- [Refresh Rate] (リフレッシュ レート) – ターゲット サーバのリフレッシュ レートです。
- [Protocol Version] (プロトコル バージョン) – Raritan 通信プロトコル バージョンです。

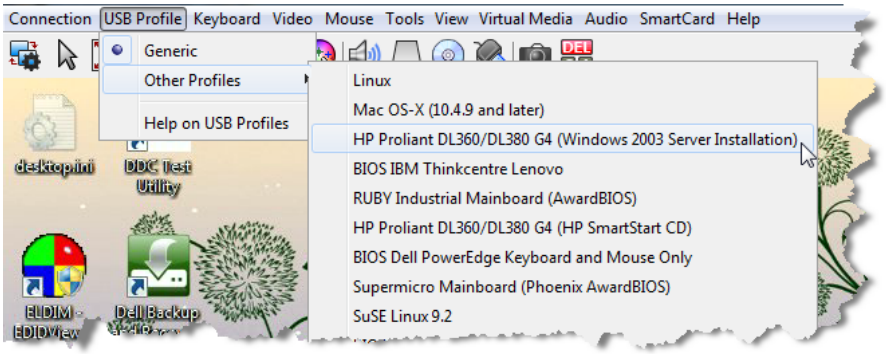
接続情報のアクセスおよびコピー



手順	
1	[Connection] (接続) の [Info...] (情報...) をクリックして、[Connection] (接続) 情報ダイアログ ボックスを開きます。
2	[Copy to Clipboard] (クリップボードにコピー) をクリックします。選択したファイルに情報を貼り付けます。

USB プロファイル

Virtual KVM Client (VKC) でターゲット サーバの USB プロファイルを設定するには、メニューの [USB Profile] (USB プロファイル) をクリックして、メニュー項目を選択します。



KVM ターゲット サーバに最適な USB プロファイルを選択します。

たとえば、サーバで Windows® オペレーティング システムが実行されている場合は、Generic プロファイルが最適です。

あるいは、BIOS メニューの設定の変更または仮想メディア ドライブからの起動を行う場合、ターゲット サーバ モデルによっては、BIOS プロファイルの方が適している可能性があります。

USB プロファイルの詳細については、オンライン ヘルプの「**USB プロファイル**（USB Profiles）『49p. の"**USB プロファイル**"参照 』」を参照してください。

キーボード

[Send Ctrl+Alt+Del] (Ctrl+Alt+Del の送信) マクロ

Ctrl+Alt+Delete マクロは、頻繁に使用されるため事前にプログラムされています。

[Keyboard]（キーボード）の [Send Ctrl+Alt+Del]（Ctrl+Alt+Del の送信）を選択するか、ツール バーの [Ctrl+Alt+Delete] ボタン をクリックすると、現在接続中のサーバまたは KVM スイッチにこのキー操作が送信されます。

一方、Ctrl キー、Alt キー、Delete キーを同時に押すと、Windows オペレーティング システムの構造により、コマンドはターゲット サーバへ送信されずに操作中の PC に適用されます。

[Send LeftAlt+Tab] (Send LeftAlt+Tab の送信)

[Keyboard]（キーボード）の [Send LeftAlt+Tab]（Send LeftAlt+Tab の送信）を選択して、接続先のターゲット サーバまたは KVM スイッチの開かれているウィンドウを切り替えます。

CIM キーボード/マウス オプションの設定

▶ DCIM-USBG2 の設定メニューにアクセスするには、以下の手順に従います。

1. Windows® のメモ帳などのウィンドウにマウス ポインタを置きます。
2. [Set CIM Keyboard/Mouse options]（CIM キーボード/マウス オプションを設定する）を選択します。この操作は、左 Ctrl + Num Lock キーをターゲットに送信することと同じです。CIM セットアップ メニュー オプションが表示されます。
3. 言語とマウスを設定します。
4. メニューを終了し、通常の CIM 機能に戻ります。

[Send Text to Target] (テキストをターゲットに送信)

▶ マクロでテキストをターゲットに送信する機能を使用するには、以下の手順に従います。

1. [Keyboard] (キーボード) の [Send Text to Target] (テキストをターゲットに送信) をクリックします。[Send Text to Target] (テキストをターゲットに送信) ダイアログ ボックスが表示されます。
2. ターゲットに送信するテキストを入力します。

注:テキストをターゲットに送信する機能では、英語以外の文字はサポートされていません。

3. ターゲットで英語 (アメリカ)/インターナショナル キーボード レイアウトが使用されている場合は、[Target system is set to the US/International keyboard layout] (ターゲットシステムで英語 (アメリカ)/インターナショナル キーボード レイアウトを使用) チェックボックスをオンにします。
4. [OK] をクリックします。

キーボード マクロ

キーボード マクロを利用することで、ターゲット サーバに対するキー入力が確実にターゲット サーバに送信され、ターゲット サーバのみで解釈されます。キーボード マクロを利用しない場合、Virtual KVM Client が実行されているコンピュータ (クライアント PC) によって解釈される可能性があります。

マクロはクライアント PC に保存され、その PC 専用になります。したがって、別の PC を使用したときは、作成したマクロを使用できません。

さらに、キーボード マクロはコンピュータ単位で管理されるので、あるユーザが使用している PC に別のユーザが自分の名前でログインした場合でも、1 人目のユーザが作成したマクロが 2 人目のユーザに対して表示されます。

Virtual KVM Client (VKC) で作成されたキーボード マクロは、Active KVM Client (AKC) では使用できません。また、その逆も同様です。

マクロの新規作成

▶ マクロを作成するには、以下の手順に従います。

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) をクリックします。[Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。
2. [Add] (追加) をクリックします。[Add Keyboard Macro] (キーボード マクロの追加) ダイアログ ボックスが表示されます。

3. [Keyboard Macro Name] (キーボード マクロ名) フィールドにマクロの名前を入力します。この名前は、マクロが作成された後に [Keyboard] (キーボード) メニューに表示されます。
4. [Hot-Key Combination] (ホットキーの組み合わせ) フィールドで、ドロップダウン リストからキー操作の組み合わせを選択します。これにより、定義済みのキー入力でマクロを実行できます。**(オプション)**
5. [Keys to Press] (押すキー) ドロップダウン リストで、コマンドの実行に使用されるキー操作のエミュレート用のキーを選択します。キーは、押す順番で選択します。1 つ選択するごとに、[Add Key] (キーを追加) を選択します。キーを選択するごとに、[Macro Sequence] (マクロ シーケンス) フィールドに表示されます。また、1 つ選択するごとに、その [Release Key] (キーのリリース) コマンドが自動的に追加されます。

   たとえば、左 Ctrl + Esc キーを選択してウィンドウを閉じるマクロを作成します。これは、[Macro Sequence] (マクロ シーケンス) ボックスに以下のように表示されます。

   [Press Left Alt] (左 Alt の押下)

   [Press F4] (F4 の押下)

   ESC

   [Release F4] (F4 のリリース)

   ESC

   [Release Left Alt] (左 Alt のリリース)
6. [Macro Sequence] (マクロ シーケンス) フィールドで、マクロ シーケンスが正しく定義されていることを確認します。
   a. キー操作の 1 つの手順を削除するには、手順を選択して [Remove] (削除) をクリックします。
   b. キー操作の手順の順番を変更するには、手順をクリックし、上向きまたは下向きの矢印ボタンを使用して必要に応じて並べ替えます。
7. [OK] をクリックしてマクロを保存します。[Clear] (クリア) をクリックすると、すべてのフィールドがクリアされ、最初の状態に戻ります。[OK] をクリックすると [Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが現れ、新しいキーボード マクロがリスト表示されます。
8. [Close] (閉じる) をクリックして、[Keyboard Macro] (キーボード マクロ) ダイアログ ボックスを閉じます。マクロがアプリケーションの [Keyboard] (キーボード) メニューに表示されます。
9. マクロを実行するには、メニューで新しいマクロを選択するか、マクロに割り当てたキー操作を使用します。

マクロのインポート

▶ マクロをインポートするには、以下の手順に従います。

1. [Keyboard] (キーボード) の [Import Keyboard Macros] (キーボード マクロのインポート) をクリックして、[Import Macros] (マクロのインポート) ダイアログ ボックスを開きます。マクロ ファイルがあるフォルダに移動します。
2. マクロ ファイルをクリックし、[Open] (開く) をクリックしてマクロをインポートします。
   a. ファイル内のマクロ数が多い場合は、エラー メッセージが表示され、[OK] を選択するとインポートが中断されます。
   b. インポートが失敗した場合は、エラー ダイアログ ボックスが表示され、失敗した理由についてのメッセージが表示されます。[OK] をクリックすると、インポートできなかったマクロをスキップしてインポートが続行されます。
3. インポートするマクロを、それに対応するチェックボックスをオンにするか、[Select All] (すべて選択) または [Deselect All] (すべて選択解除) オプションを使用して選択します。
4. [OK] をクリックしてインポートを開始します。
   a. 重複するマクロが見つかった場合は、[Import Macros] (マクロのインポート) ダイアログ ボックスが表示されます。以下のいずれかの手順に従います。

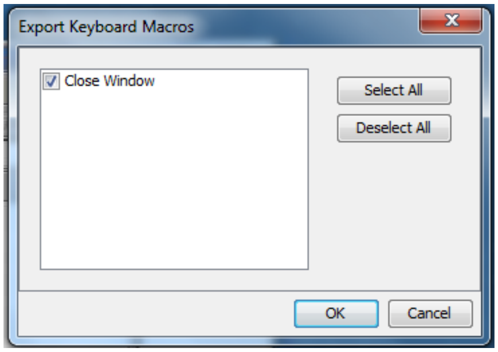
- [Yes] (はい) をクリックして、既存のマクロを、インポートしたマクロで置き換えます。
- [Yes to All] (すべてはい) をクリックして、現在選択されているマクロとその他に見つかった重複マクロすべてを置き換えます。
- [No] (いいえ) をクリックすると、元のマクロが維持され、次のマクロに進みます。
- [No to All] (すべていいえ) をクリックすると、元のマクロが維持され、次のマクロに進みます。その他に見つかったすべての重複マクロも同様にスキップされます。
- [Cancel] (キャンセル) をクリックすると、インポートが終了します。
- または、[Rename] (名前変更) をクリックして、マクロの名前を変更してそれをインポートします。[Rename] (名前変更) が選択された場合は、[Rename Macro] (マクロ名の変更) ダイアログ ボックスが表示されます。フィールドに新しいマクロ名を入力し、[OK] をクリックします。ダイアログ ボックスが閉じられ、処理が続行されます。入力した名前が別のマクロと重複している場合は、アラートが表示されるので、別のマクロ名を入力する必要があります。

b. インポート処理中にインポート済みマクロの許容数を超えた場合は、ダイアログ ボックスが表示されます。[OK] をクリックして、マクロのインポート試行を続行するか、[Cancel] (キャンセル) をクリックしてインポート処理を中止します。

これでマクロがインポートされます。既に存在するホットキーを含むマクロがインポートされた場合、インポートされたマクロのホットキーが破棄されます。

マクロのエクスポート

1. [Tools] (ツール) の [Export Macros] (マクロのエクスポート) を選択して、[Select Keyboard Macros to Export] (エクスポートするキーボード マクロの選択) ダイアログ ボックスをクリックします。



2. エクスポートするマクロを、それに対応するチェックボックスをオンにするか、[Select All] (すべて選択) または [Deselect All] (すべて選択解除) オプションを使用して選択します。
3. [OK] (OK) をクリックします。[Export Keyboard Macros] (キーボードマクロのエクスポート) ダイアログ ボックスが表示されます。マクロ ファイルを探して選択します。デフォルトでは、マクロはデスクトップにあります。
4. マクロ ファイルを保存するフォルダを選択し、ファイル名を入力し、[Save] (保存) をクリックします。マクロが既に存在する場合は、警告メッセージが表示されます。
5. [Yes] (はい) を選択して既存のマクロを上書きするか、[No] (いいえ) をクリックしてマクロを上書きせずに警告を閉じます。

ビデオのプロパティ

画面を更新する

[Refresh Screen] (画面の更新) コマンドを使用すると、ビデオ画面が更新されます。ビデオの設定を自動的に更新する方法はいくつかあります。

- [Refresh Screen] (画面の更新) コマンドを使用すると、ビデオ画面が更新されます。
- [Auto-sense Video Settings] (ビデオ設定の自動検出) コマンドを使用すると、ターゲット サーバのビデオ設定が自動的に検出されます。
- [Calibrate Color] (色調整) コマンドを使用すると、ビデオの表示色が調整されます。

これに加え、[Video Settings] (ビデオ設定) コマンドを使用すると、手動で設定を調整できます。

▶ ビデオ設定を更新するには、次のいずれかの手順に従います。

- [Video] (ビデオ) の [Refresh Screen] (画面の更新) を選択するか、ツールバーの [Refresh Screen] (画面の更新) ボタン をクリックします。

[Auto-sense Video Settings] (ビデオ設定の自動検出)

[Auto-sense Video Settings] (ビデオ設定の自動検出) コマンドを使用すると、ビデオ設定 (解像度、垂直走査周波数) が再検出され、ビデオ画面が再描画されます。

▶ **ビデオ設定を自動的に検出するには、以下の手順に従います。**

- [Video] (ビデオ) の [Auto-sense Video Settings] (ビデオ設定の自動検出) を選択するか、ツールバーの [Auto-sense Video Settings] (ビデオ設定の自動検出) ボタン をクリックします。
  調整が行われていることを示すメッセージが表示されます。

色の調整

[Calibrate Color] (色調整) コマンドは、送信されたビデオ画像の色レベル (色相、輝度、彩度) を最適化するために使用します。色設定は、ターゲット サーバごとに適用されます。

注: [Calibrate Color] (色調整) コマンドは、現在の接続のみに適用されます。

▶ **色を調整するには、以下の手順に従います。**

- [Video] (ビデオ) の [Calibrate Color] (色調整) を選択するか、ツールバーの [Calibrate Color] (色調整) ボタン をクリックします。
  ターゲット デバイス画面の色が調整されます。

ビデオ設定の調整

[Video Settings] (ビデオ設定) コマンドを使用すると、ビデオ設定を手動で調整できます。

▶ **ビデオ設定を変更するには、以下の手順に従います。**

1. [Video] (ビデオ)、[Video Settings] (ビデオ設定) を選択して、[Video Settings] (ビデオ設定) ダイアログ ボックスを開きます。
2. 必要に応じて、以下の設定を調整します。設定を調整すると、その効果が即座に表示に反映されます。
   a. [PLL Settings] (PLL 設定)
      [Clock] (クロック) - ビデオ画面上にビデオ ピクセルが表示される速度を制御します。クロック設定値を変更すると、ビデオ画像が水平方向に伸縮します。設定値は奇数を推奨します。通常は自動検出機能によって適切に設定されるため、ほとんどの環境ではこの設定を変更する必要はありません。

[Phase] (位相) – 位相の値の範囲は 0 ～ 31 です。これより大きな値は反復されます。アクティブなターゲット サーバ用に最適なビデオ画像が得られる位相の位置で停止してください。

b. [Brightness] (明るさ): この設定は、ターゲット サーバの画面表示の輝度を調整するために使用します。
c. [Brightness Red] (赤輝度) – ターゲット サーバの画面に表示される赤の信号の輝度を制御します。
d. [Brightness Green] (緑輝度) – 緑の信号の輝度を制御します。
e. [Brightness Blue] (青輝度) – 青の信号の輝度を制御します。
f. [Contrast Red] (赤コントラスト) – 赤の信号のコントラストを制御します。
g. [Contrast Green] (緑コントラスト) – 緑の信号のコントラストを制御します。
h. [Contrast Blue] (青コントラスト) – 青の信号のコントラストを制御します。

ビデオ画像が大幅にぼやけている場合、設定でクロックと位相を調節することで、アクティブなターゲット サーバの画像を改善します。

警告: クロック設定と位相設定を変更する際には、注意が必要です。ビデオ画像が消えたり歪んだりする可能性があるだけでなく、元の状態に戻せなくなることがあります。変更を加える前に、ラリタン テクニカル サポートにお問い合わせください。

---

i. [Horizontal Offset] (水平オフセット) – ターゲット サーバの画面がモニタに表示されるときの水平位置を制御します。
j. [Vertical Offset] (垂直オフセット) – ターゲット サーバの画面がモニタに表示されるときの垂直位置を制御します。

3. [Automatic Color Calibration] (自動色調節) を選択して、この機能を有効にします。
4. ビデオ検出モードを選択します。
   - [Best possible video mode] (最適ビデオ モード)

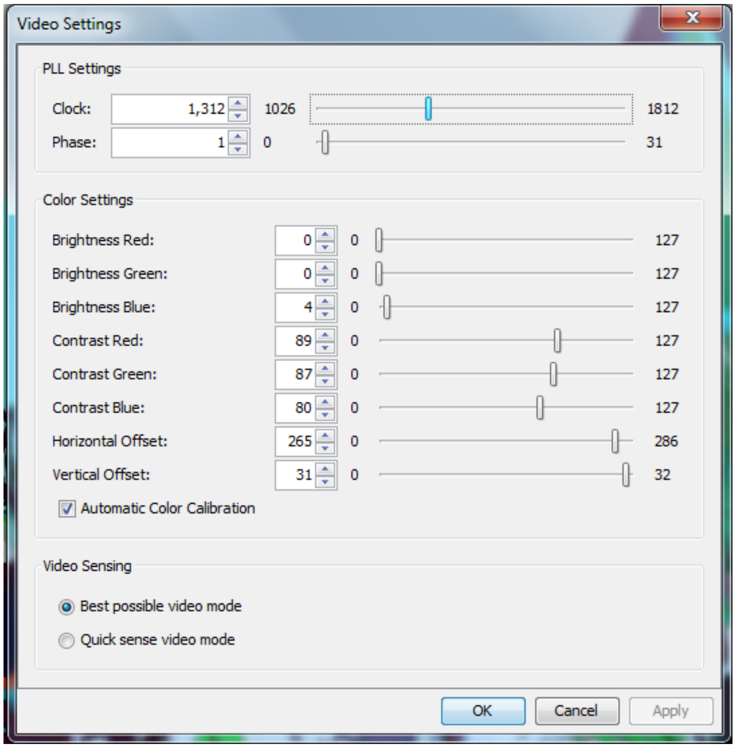
   ターゲットやターゲットの解像度が変更されたときに、すべての自動検出処理が実行されます。このオプションを選択すると、最適な画像品質になるようにビデオが調整されます。

   - [Quick sense video mode] (クイック検出ビデオ モード)

   このオプションを使用すると、クイック ビデオ自動検出が使用され、ターゲットのビデオがより早く表示されます。このオプションは、再起動直後のターゲット サーバの BIOS 設定を入力するときに特に有効です。

5. 設定を適用してダイアログ ボックスを閉じるには、[OK] をクリックします。ダイアログ ボックスを閉じずに設定を適用するには、[Apply] (適用) をクリックします。

注: 一部の Sun サーバでは、ある種の Sun 背景画面 (外周部が非常に暗いものなど) が中央の位置に正確に表示されない場合があります。別の背景を使用するか、画面の左上隅に明るい色のアイコンを配置してください。



ターゲット コマンドによるスクリーンショット (ターゲット スクリーンショット)

[Screenshot from Target server] (ターゲット サーバのスクリーンショット) コマンドを使用すると、ターゲット サーバのスクリーンショットを取得できます。必要に応じて、このスクリーンショットを、選択した場所にビットマップ、JPEG、または PNG ファイルとして保存します。

▶ ターゲット サーバのスクリーンショットを取得するには、以下の手順に従います。

1. [Video] (ビデオ) の [Screenshot from Target server] (ターゲット サーバのスクリーンショット) を選択するか、ツールバーの [Target Screenshot] (ターゲット スクリーンショット) ボタン をクリックします。
2. [Save] (保存) ダイアログ ボックスで、ファイルを保存する場所を選択し、ファイルに名前を付け、[Files of type] (ファイルの種類) ドロップダウン リストからファイル形式を選択します。

3. [Save] (保存) をクリックしてスクリーンショットを保存します。

マウス オプション

デュアル マウス モードでオプションが適切に設定されている場合、2 つのマウス カーソルは同調します。

デュアル マウス モードで、ターゲット サーバを制御しているとき、リモート コンソールには、2 つのマウス カーソルが表示されます。1 つは KX III クライアント ワークステーションのマウス カーソルで、もう 1 つはターゲット サーバのマウス カーソルです。

この場合、シングル マウス モードとデュアル マウス モードのどちらかを使用できます。

デバイスでは、2 つのマウス カーソルが存在するときに以下のマウス モードが提供されます。

- Absolute (ずれない) (マウス同期)
- Intelligent (インテリジェント) (マウス モード)
- Standard (標準) (マウス モード)

マウス ポインタが KVM Client ターゲット サーバ ウィンドウ内にある場合、マウスの動作やクリックは、接続されているターゲット サーバに直接送信されます。

クライアントのマウス ポインタは、マウスの加速設定により、動作がわずかにターゲット マウス ポインタより先行します。

高速 LAN 接続では、シングル マウス モードでターゲット サーバのポインタのみを表示できます。

この 2 つのモード (シングル マウスとデュアル マウス) は自由に切り替えることができます。

デュアル マウス モード

ずれないマウス モード

このモードでは、ターゲット マウスの加速または速度が異なる値に設定されている場合でも、クライアントとターゲットのカーソルを同期するために絶対座標が使用されます。

このモードは USB ポートを備えたサーバでサポートされ、仮想メディア CIM のデフォルトのモードです。

ずれないマウス モード では、仮想メディア CIM を使用する必要があります。

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

▶ **ずれないマウス モードに切り替えるには、以下の手順に従います。**

- [Mouse] (マウス) の [Absolute] (ずれない) を選択します。

キーボードおよびマウスには、DVUSB CIM の黒のコネクタが使用されています。グレーのコネクタは、仮想メディアに使用します。

CIM の両方のプラグをデバイスに接続したままにします。両方のプラグがターゲット サーバに接続されていない場合は、デバイスが正しく動作しないことがあります。

インテリジェント マウス モード

デバイスでは、インテリジェント マウス モードにおいて、ターゲットのマウス設定を検出し、それに応じてマウス カーソルを同期できるので、ターゲットでマウスの加速を設定できます。インテリジェント マウス モードは、VM ターゲット以外のデフォルトです。

インテリジェント マウス モードへの切り替え

▶ **インテリジェント マウス モードに切り替えるには、以下の手順に従います。**

- [Mouse] (マウス) の [Intelligent] (インテリジェント) を選択します。

インテリジェント マウス同期の条件

[Mouse] (マウス) メニューにある [Intelligent Mouse Synchronization] (インテリジェント マウス同期) コマンドを選択すると、マウスが動いていないときにマウス カーソルが自動的に同期されます。この機能を適切に動作させるには、次の条件が満たされている必要があります。

- ターゲットにおいて、アクティブ デスクトップが無効であること。
- ターゲット ページの左上隅にウィンドウが表示されていないこと。
- ターゲット ページの左上隅にアニメーション背景が表示されていないこと。
- ターゲットのマウス カーソルが通常のものであり、アニメーション カーソルでないこと。
- ターゲット マウスの速度が、非常に遅い値や非常に速い値に設定されていないこと。
- [ポインタの精度を高める] や [ポインタを自動的に既定のボタン上に移動する] などの高度なマウス プロパティが無効であること。
- [ビデオ設定] ウィンドウで [最適ビデオ モード] を選択していること。
- ターゲットのビデオの外周部が明確に表示されていること (つまり、ターゲットのビデオ画像の端にスクロールしたときに、ターゲット デスクトップとリモート KVM コンソール ウィンドウの間に黒いボーダーが表示されている必要があります)。
- インテリジェント マウス同期機能を使用中に、デスクトップの左上隅にファイル アイコンやフォルダ アイコンがあると、この機能が正しく動作しない可能性があります。この機能での問題を避けるために、デスクトップの左上隅にファイル アイコンやフォルダ アイコンを置かないことを推奨します。

ターゲット ビデオが自動検出された後で、ツール バーの [Synchronize Mouse] (マウス同期) ボタンをクリックして、手動でマウス同期を開始する必要があります。ターゲットの解像度が変更された場合や、マウス カーソルが互いに同期しなくなった場合にも、この操作を行います。

インテリジェント マウス同期が失敗した場合、標準マウス同期と同じ動作になります。

マウス設定は、ターゲットのオペレーション システムよって異なります。詳細については、使用する OS のマニュアルを参照してください。また、インテリジェント マウス同期は UNIX ターゲットでは機能しません。

標準マウス モード

標準マウス モードは、相対マウス位置を使用した標準のマウス同期アルゴリズムです。標準マウス モードを使用する場合、クライアントとサーバのカーソルが同期するように、マウスの加速を無効にし、マウスに関連するその他のパラメータを適切に設定する必要があります。

▶ **標準マウス モードに切り替えるには、以下の手順に従います。**

- [Mouse] (マウス) の [Standard] (標準) を選択します。

マウス同期のヒント

マウス同期に問題がある場合は、以下の手順に従います。

1. 選択したビデオ解像度と垂直走査周波数がデバイスでサポートされていることを確認します。[KVM Client Connection Info] (KVM Client 接続情報) ダイアログ ボックスには、デバイスの表示で使用している実際の値が表示されます。
2. [KVM Client auto-sense] (KVM Client の自動検出) ボタンをクリックして自動検出を強制します。
3. 以上の手順で Linux、UNIX、Solaris KVM ターゲット サーバのマウス同期が改善しない場合は、以下の手順に従います。
   a. ターミナル ウィンドウを開きます。
   b. 次のコマンドを入力します。`xset mouse 1 1`
   c. ターミナル ウィンドウを閉じます。
4. [KVM Client mouse synchronization] (KVM Client マウス同期) ボタン をクリックします。

マウスの同期

デュアル マウス モードで [Synchronize Mouse] (マウスの同期) コマンドを使用すると、ターゲット サーバのマウス ポインタと KVM Client のマウス ポインタとの同期化が再実行されます。

▶ **マウスを同期するには、次のいずれかの手順に従います。**

- [Mouse] (マウス) の [Synchronize Mouse] (マウスの同期) を選択するか、ツールバーの [Synchronize Mouse] (マウスの同期) ボタン をクリックします。

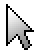
注:このオプションは、標準マウス モードとインテリジェント マウス モードでのみ使用可能です。

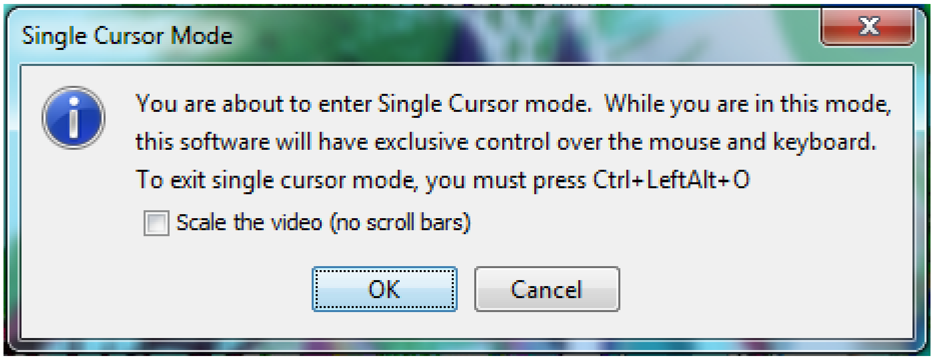
シングル マウス モード

シングル マウス モードでは、ターゲット サーバのマウス カーソルだけを使用します。ローカル マウス ポインタは画面に表示されません。

注:クライアントが仮想マシン上で実行している場合、シングル マウス モードは Windows および Linux のターゲットでは機能しません。

▶ シングル マウス モードにするには、次のいずれかの手順に従います。

- [Mouse] (マウス) の [Single Mouse Cursor] (シングル マウス カーソル) を選択します。
- ツール バーの [Single/Double Mouse Cursor] (シングル/ダブル マウス カーソル) ボタン  をクリックします。



▶ シングル マウス モードを終了するには、以下の手順に従います。

1. シングル マウス モードを終了するには、キーボードの Ctrl+Alt+O を押します。

ツール オプション

[General Settings] (全般)

▶ ツール オプションを設定するには、以下の手順に従います。

1. [Tools] (ツール) メニューの [Options] (オプション) を選択します。[Options] (オプション) ウィンドウが表示されます。
2. テクニカル サポートから指示されたときだけ、[Enable Logging] (ログ記録を有効にする) チェックボックスをオンにします。

   このオプションをオンにすると、ホーム ディレクトリにログ ファイルが作成されます。
3. 必要に応じて、ドロップダウン リストからキーボードの種類を選択します。

含まれるオプションは次のとおりです。

- [US/International] (アメリカ英語/国際)
- [French (France)] (フランス語 (フランス))
- [German (Germany)] (ドイツ語 (ドイツ))
- 日本語
- [United Kingdom] (イギリス英語)
- [Korean (Korea)] (韓国語 (韓国))
- [French (Belgium)] (フランス語 (ベルギー))
- [Norwegian (Norway)] (ノルウェー語 (ノルウェー))
- [Portuguese (Portugal)] (ポルトガル語 (ポルトガル))
- [Danish (Denmark)] (デンマーク語 (デンマーク))
- [Swedish (Sweden)] (スウェーデン語 (スウェーデン))
- [German (Switzerland)] (ドイツ語 (スイス))
- [Hungarian (Hungary)] (ハンガリー語 (ハンガリー))
- [Spanish (Spain)] (スペイン語 (スペイン))
- [Italian (Italy)] (イタリア語 (イタリア))
- スロベニア語
- [Translation: French - US] (変換: フランス語 - アメリカ英語)
- [Translation: French - US International] (変換: フランス語 - アメリカ英語/国際)

AKC では、デフォルトのキーボードの種類はローカル クライアントであるため、このオプションは適用されません。

4. ホットキーを設定します。
   - [Exit Full Screen Mode - Hotkey] (全画面モードの終了 - ホットキー)。

     全画面モードに切り替えると、ターゲット サーバの表示が全画面表示になり、ターゲット サーバと同じ解像度が取得されます。

     これは、このモードを終了するためのホットキーです。
   - [Exit Single Cursor Mode - Hotkey] (シングル カーソル モードの終了- ホットキー)。

     シングル カーソル モードに入ると、ターゲット サーバのマウス カーソルのみが表示されます。

     これは、シングル カーソル モードを終了して、クライアント マウス カーソルに戻るために使用するホットキーです。
   - [Disconnect from Target - Hotkey] (ターゲットから切断 - ホットキー)。

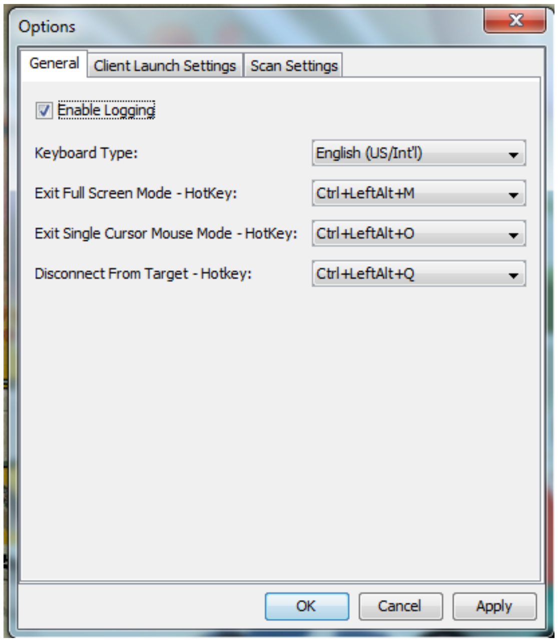
     このホットキーを有効にすると、ターゲットからすばやく切断できます。

アプリケーションでは、同じホットキーの組み合わせを複数の機能に割り当てることはできません。

たとえば、Q が既に [Disconnect from Target] (ターゲットから切断) 機能に割り当てられている場合、それを [Exit Full Screen Mode] (全画面モードの終了) 機能に割り当てることはできません。

さらに、ホットキーがアップグレードによってアプリケーションに追加されたときにそのキーのデータ値が既に使用されていた場合は、次に利用できる値が、代わりにその機能に適用されます。

5. [OK] をクリックします。



キーボードの制限

トルコ語キーボード

トルコ語のキーボードを使用している場合は、Active KVM Client (AKC) を介してターゲット サーバに接続する必要があります。他の Raritan クライアントではサポートされていません。

スロベニア語キーボード

JRE の制限により、< キーは、スロベニア語キーボードでは機能しません。

Linux での言語設定

Linux 上の Sun JRE では、システムの環境設定を使用して設定される外国語のキーボードで正しいキー イベントを生成する際に問題があるので、外国語キーボードは、次の表で説明する方法を使用して設定することをお勧めします。

言語	設定方法
アメリカ英語/国際	デフォルト設定
フランス語	Keyboard Indicator
ドイツ語	[System Settings] (システム設定) (Control Center)
日本語	[System Settings] (システム設定) (Control Center)
イギリス英語	[System Settings] (システム設定) (Control Center)
韓国語	[System Settings] (システム設定) (Control Center)
ベルギー語	Keyboard Indicator
ノルウェー語	Keyboard Indicator
デンマーク語	Keyboard Indicator
スウェーデン語	Keyboard Indicator
ハンガリー語	[System Settings] (システム設定) (Control Center)
スペイン語	[System Settings] (システム設定) (Control Center)
イタリア語	[System Settings] (システム設定) (Control Center)
スロベニア語	[System Settings] (システム設定) (Control Center)
ポルトガル語	[System Settings] (システム設定) (Control Center)

注: デスクトップ環境として Gnome を使用している Linux システムでは、Keyboard Indicator を使用してください。

クライアント起動設定

クライアント起動設定をカスタマイズすると、KVM セッションにおける画面設定を定義できます。

▶ **クライアント起動設定をカスタマイズするには、以下の手順に従います。**

1. [Tools] (ツール) メニューの [Options] (オプション) を選択します。[Options] (オプション) ウィンドウが表示されます。
2. [Client Launch Settings] (クライアント起動設定) タブをクリックします。
   - ターゲット ウィンドウ設定をカスタマイズするには

a. ターゲットの現在の解像度に合ったサイズのウィンドウを開くには、[Standard - sized to target Resolution] (標準 ― ターゲットの解像度に合わせる) を選択します。ターゲットの解像度がクライアントの解像度よりも高い場合、画面全体にターゲット ウィンドウが表示され、表示しきれない部分がある場合は、スクロール バーが追加表示されます。

b. ターゲット ウィンドウを全画面モードで開くには、[Full Screen] (全画面) を選択します。

- ターゲット ビューアが起動するモニタをカスタマイズするには

a. クライアント上で使用されているアプリケーション (例: Web ブラウザ、アプレット) を表示しているモニタでターゲット ビューアを起動するには、[Monitor Client Was Launched From] (クライアントが起動されているモニタ) を選択します。

b. アプリケーションによって現在検出されているモニタの一覧から選択するには、[Select From Detected Monitors] (検出されたモニタの中から選択) を選択します。以前選択したモニタが検出されなくなった場合、"Currently Selected Monitor Not Detected" (現在選択されているモニタが検出されませんでした) というメッセージが表示されます。

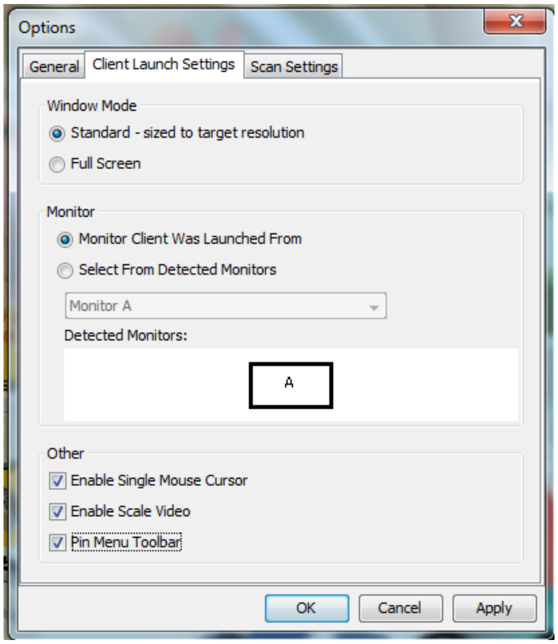
- 追加の起動設定をカスタマイズするには、以下の手順に従います。

a. サーバにアクセスされたときにデフォルト マウス モードとしてシングル マウス モードを有効にするには、[Enable Single Cursor Mode] (シングル カーソル モードを有効にする) を選択します。

b. ターゲット サーバにアクセスされたときに、表示サイズを自動的に拡大、縮小するには、[Enable Scale Video] (ビデオの拡大、縮小を有効にする) 選択します。

c. 全画面モードの場合でもターゲットのツールバーを表示したままにする場合は、[Pin Menu Toolbar] (メニュー ツールバーを常に表示) を選択します。デフォルトでは、ターゲットが全画面モードの場合、メニューは、マウスを画面上部に移動した場合にのみ表示されます。

3. ［OK］をクリックします。



VKC および AKC でのポート スキャンの設定

VKC および AKC でのポート スキャンの設定は、KX III リモート コンソールからのスキャンに適用されます。

ローカル コンソールのポート スキャン オプションを設定するには、「*ローカル コンソール スキャンの設定* 『*305*p. 』」を参照してください。

選択したターゲットを検索してそれをスライド ショー ビューで表示するポート スキャン機能を使用すると、最大 32 のターゲットを一度にモニタできます。

ターゲットに接続することも、必要に応じて特定のターゲットをフォーカスすることもできます。スキャン対象は、標準ターゲット、ブレード サーバ、カスケード接続 Dominion デバイス、KVM スイッチの各ポートです。

Virtual KVM Client (VKC) または Active KVM Client (AKC) からスキャン設定を指定します。

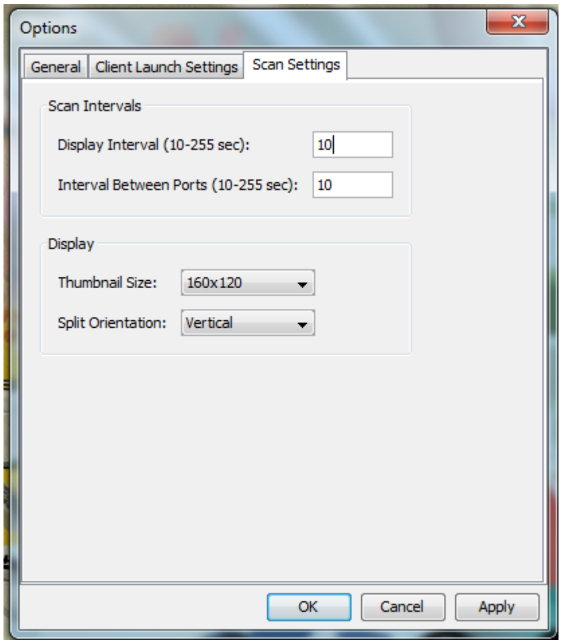
「ポートのスキャン － リモート コンソール」を参照してください。

[Scan Settings]（スキャン設定）タブを使用して、スキャン間隔およびデフォルト表示オプションをカスタマイズします。

ポート スキャンの設定

▶ スキャン設定をカスタマイズするには、以下の手順に従います。

1. [ツール] メニューの [オプション] を選択します。[オプション] ウィンドウが表示されます。
2. [スキャン設定] タブを選択します。
3. [表示間隔 (10 ～ 255 秒):]: フィールドで、フォーカスを持つターゲットを [ポート スキャン] ウィンドウの中央に表示する秒数を指定します。
4. [Interval Between Ports (10 - 255 sec):] (ポート間の間隔 (10 ～ 255 秒):) フィールドで、ポート間でデバイスを一時停止する間隔を指定します。
5. [表示] セクションで、[ポート スキャン] ウィンドウのサムネイルのサイズと分割方向のデフォルト表示オプションを変更します。
6. [OK] をクリックします。



表示オプション

[View Toolbar] (ツール バーの表示)

Virtual KVM Client では、ツール バーの表示/非表示を切り替えることができます。

▶ **ツール バーの表示/非表示 (オン/オフ) を切り替えるには、以下の手順に従います。**

- [View] (表示) の [View Toolbar] (ツール バーの表示) を選択します。

[View Status Bar] (ステータス バーの表示)

デフォルトでは、ステータス バーはターゲット ウィンドウの下部に表示されます。

▶ **ステータス バーを非表示にするには、以下の手順に従います。**

- [View] (表示) の [Status Bar] (ステータス バー) をクリックして選択解除します。

▶ **ステータス バーを復元するには、以下の手順に従います。**

- [View] (表示) の [Status Bar] (ステータス バー) をクリックして選択します。

[Scaling] (拡大、縮小)

ターゲットのウィンドウを拡大、縮小することで、ターゲット サーバ ウィンドウ全体の内容を表示することができます。

Virtual KVM Client のウィンドウ サイズに合わせて、縦横比を維持したまま、ターゲット ビデオのサイズを拡大または縮小することができるため、スクロール バーを使用することなくターゲット サーバのデスクトップ全体を表示することができます。

▶ **拡大、縮小 (オン/オフ) を切り替えるには、以下の手順に従います。**

- [View] (表示) の [Scaling] (拡大、縮小) を選択します。

[Full Screen Mode] (全画面モード)

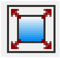
全画面モードに切り替えると、ターゲットの全画面が表示され、ターゲット サーバと同じ解像度になります。

このモードを終了するためのホットキーは、[Options] (オプション) ダイアログ ボックスで指定します。「***ツール オプション*** 『*263*p. 』」を参照してください。

全画面モードになっているときに、マウス ポインタを画面上端に移動すると、全画面モード メニュー バーが表示されます。

全画面モードの場合でもメニュー バーを表示したままにする場合は、[Tool] (ツール) の [Options] (オプション) ダイアログ ボックスの [Pin Menu Toolbar] (メニュー ツールバーを常に表示] を有効にします。「***ツール オプション*** 『*263*p. 』」を参照してください。

▶ 全画面モードに切り替えるには、以下の手順に従います。

- [View] (表示) の [Full Screen] (全画面) を選択するか、[Full Screen] (全画面) ボタン  をクリックします。

▶ 全画面モードを終了するには、以下の手順に従います。

- [Tool] (ツール) の [Options] (オプション) ダイアログで設定されているホットキーを押します。デフォルトは Ctrl+Alt+M です。

常に全画面モードの状態でターゲットにアクセスしたい場合、全画面モードをデフォルトにすることができます。

▶ 全画面モードをデフォルトに設定するには

1. [Tools] (ツール) メニューの [Options] (オプション) をクリックし、[Options] (オプション) ダイアログ ボックスを開きます。
2. [Enable Launch in Full Screen Mode] (全画面モードで起動する) を選択し、[OK] (OK) をクリックします。

仮想メディア

すべての KX III モデルにおいて仮想メディアがサポートされています。KVM の機能を拡張する仮想メディアにより、クライアント PC やネットワーク ファイル サーバ上のメディアにリモートのターゲット サーバからアクセスできるようになります。

この機能を使用すると、クライアント PC やネットワーク ファイル サーバでマウントされたメディアが、ターゲット サーバでも仮想的にマウントされます。これにより、そのメディアはターゲット サーバ自体に物理的に接続されているような形で読み書きできるようになります。

それぞれの KX III は仮想メディアに対応しているので、CD、DVD、USB、音声再生および録音デバイス、内部およびリモート ドライブ、イメージなどのいろいろなデバイスを使用したリモート管理タスクが可能です。

仮想メディアのセッションは、128 または 256 ビットの AES または RC4 暗号化によって保護されます。

仮想メディアを使用するための条件

KX III の前提条件

- 仮想メディアへのアクセスを要求するユーザに対して、該当するポートへのアクセスや、これらのポートの仮想メディア アクセス（VM アクセス ポート権限）を許可するように KX III を設定する必要があります。ポート権限はグループレベルで設定されます。
- デバイスとターゲット サーバ間に USB 接続が存在する必要があります。
- PC 共有を使用する場合は、[Security Settings]（セキュリティ設定）ページでセキュリティ設定を有効にする必要があります。**(オプション)**
- 接続先の KVM ターゲット サーバの適切な USB プロファイルを選択する必要があります。

リモート PC

- 仮想メディアの一部のオプションを使用するには、リモート PC に対する管理者特権が必要です（ドライブ全体のドライブ リダイレクト機能など）。

注:Microsoft Vista または Windows 7 を使用している場合は、[ユーザアカウント制御] を無効にするか、Internet Explorer を起動するときに [管理者として実行] を選択しますこのためには、[スタート] メニューの [Internet Explorer] を右クリックし、[管理者として実行] を選択します。

ターゲット サーバ

- KVM ターゲット サーバは USB 接続のドライブをサポートする必要があります。
- USB 2.0 ポートの方が高速なため、推奨されます。

仮想メディアに必要な CIM

次のいずれかの CIM を使用して仮想メディアを利用する必要があります。

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

キーボードおよびマウスには、DVUSB CIM の黒のコネクタが使用されています。グレーのコネクタは、仮想メディアに使用します。

CIM の両方のプラグをデバイスに接続したままにします。両方のプラグがターゲット サーバに接続されていない場合は、デバイスが正しく動作しないことがあります。

ローカル ドライブのマウント

このオプションを使用すると、ドライブ全体がマウントされます。つまり、クライアントコンピュータのディスク ドライブ全体がターゲット サーバに仮想的にマウントされます。

このオプションは、ハード ディスク ドライブと外部ドライブにのみ使用してください。ネットワーク ドライブ、CD-ROM ドライブ、または DVD-ROM ドライブは対象外です。

ローカル ドライブのマウントに関する留意事項

Windows XP® オペレーティング システムが稼動している KVM ターゲット サーバでは、NTFS 形式のパーティション (ローカル C ドライブなど) がリダイレクトされた後で新しいマス ストレージ接続を行うことができない場合があります。

その場合には、リモート コンソールを閉じて再接続した後で、別の仮想メディア デバイスをリダイレクトしてください。同じターゲット サーバに別のユーザーが接続している場合、そのユーザーの接続も閉じる必要があります。

仮想メディアによりサポートされているタスク

仮想メディアを使用することで、以下のような作業をリモートから実行できるようになります。

- ファイルの転送
- 診断の実行
- アプリケーションのインストールと修正パッチ（patch）の適用
- オペレーティング システムの完全インストール
- デジタル音声の録音および再生

サポートされている仮想メディア タイプ

Windows®、Mac®、Linux™ の各クライアントでは、以下の仮想メディア タイプがサポートされています。

- 内蔵ハード ディスク ドライブおよび外付けハード ディスク ドライブ
- 内蔵または USB マウントされた CD ドライブや DVD ドライブ
- USB マス ストレージ デバイス
- PC ハード ディスク ドライブ
- ISO イメージ（ディスク イメージ）
- デジタル音声デバイス*

注:ラリタンは ISO9660 を標準でサポートしています。ただし、他の ISO 標準も使用できます。

読み取り/書き込み可能に設定できない状況

以下の場合、仮想メディアを読み取り/書き込み可能にすることはできません。

- Linux® および Mac® の各クライアント
- ドライブが書き込み保護されている場合
- ユーザに読み取り/書き込みの権限がない場合。
  - ポート権限の [Access]（アクセス）が [None]（なし）または [View]（表示）に設定されている場合。
  - ポート権限の [VM Access]（VM アクセス）が [Read-Only]（読み取り専用）または [Deny]（拒否）に設定されている場合。

サポートされている仮想メディア オペレーティング システム

サポートされているクライアント オペレーティング システムは次のとおりです。

- Windows® 7 オペレーティング システム
- Windows 8 オペレーティング システム
- Windows XP® オペレーティング システム
- openSUSE® 11.4 Celadon (x86_64)
- Fedora® 18
- RHEL® 6.4
- OSX Mountain Lion® 10.7 (以降)
- Solaris® 10

Active KVM Client (AKC) を使用して仮想メディア タイプをマウントできますが、Windows オペレーティング システムのみが対象となります。

サポートされている仮想メディア ドライブ数

仮想メディア機能を使用する場合、現在ターゲットに適用されている USB プロファイルでサポートされている異なる種類のドライブを 2 台までマウントできます。このドライブは、KVM セッションの間のみアクセスできます。

たとえば、特定の CD-ROM をマウントして、それを使用し、作業が終了したら切断することができます。それでも、別の CD-ROM を仮想的にマウントできるように、この CD-ROM 仮想メディアの "チャンネル" は開いたままになります。このような仮想メディアの "チャネル" は、USB プロファイルがサポートしている限り、KVM セッションが閉じられるまで開いたままになっています。

仮想メディアを使用するには、ターゲット サーバからアクセスできるようにするメディアを、クライアントまたはネットワーク ファイル サーバに接続します。

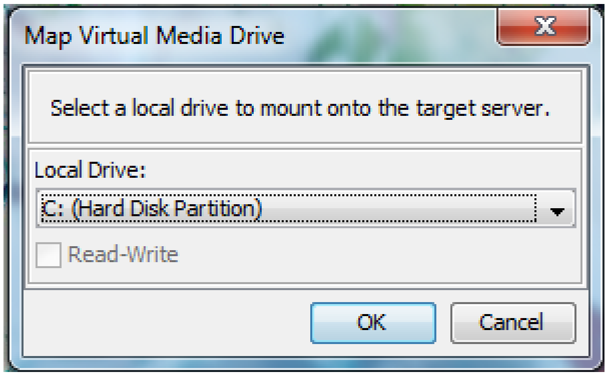
この手順を最初に行う必要はありませんが、このメディアにアクセスする前に行う必要があります。

仮想メディアの接続および切断

クライアント コンピュータの仮想メディア ドライブへのアクセス

▶ **クライアント コンピュータの仮想メディア ドライブにアクセスするには、以下の手順に従います。**

1. Virtual KVM Client で、[Virtual Media] (仮想メディア) の [Connect Drive] (ドライブの接続) を選択するか、[Connect Drive...] (ドライブの接続...) ボタン をクリックします。[Map Virtual Media Drive] (仮想メディア ドライブの割り当て) ダイアログ ボックスが表示されます。



2. [Local Drive] (ローカル ドライブ) ドロップダウン リストから、ドライブを選択します。

   読み取りと書き込みの機能が必要な場合には、[Read-Write] (読み取り/書き込み可能) チェックボックスをオンにします。

   このオプションは、リムーバブル ドライブ以外では無効になっています。詳細は、「*読み取り/書き込み可能に設定できない状況*『*274*p. 』」を参照してください。

   このチェックボックスをオンにすると、接続した USB ディスクに読み取りと書き込みを実行できるようになります。

   警告: 読み取り/書き込みアクセスを有効にすると危険な場合があります。同じドライブに対して同時に複数のクライアント PC からアクセスすると、データが壊れる恐れがあります。書き込みアクセスが不要な場合は、このオプションをオフのままにしてください。

   ---

3. [OK] をクリックします。メディアがターゲット サーバに仮想的にマウントされます。このメディアには、他のドライブとまったく同じようにアクセスすることができます。

CD-ROM/DVD-ROM/ISO イメージのマウント

このオプションを使用して、CD-ROM、DVD-ROM、ISO イメージをマウントします。

注:Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

▶ CD-ROM、DVD-ROM、ISO イメージにアクセスするには、以下の手順に従います。

1. Virtual KVM Client で、[Virtual Media] (仮想メディア) の [Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続) を選択するか、[Connect CD-ROM/ISO] (CD-ROM/ISO に接続) ボタン をクリックします。[Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックスが表示されます。
2. 内部および外部の CD-ROM ドライブまたは DVD-ROM ドライブの場合
   a. [Local CD/DVD Drive] (ローカル CD/DVD ドライブ) を選択します。
   b. [Local CD/DVD Drive] (ローカル CD/DVD ドライブ) ドロップダウン リストから、ドライブを選択します。使用可能なすべての内部/外部の CD ドライブおよび DVD ドライブの名前が、ドロップダウン リストに表示されます。
   c. [接続] をクリックします。
3. ISO イメージの場合
   a. [ISO Image] (ISO イメージ) オプションを選択します。CD、DVD、またはハード ディスクのディスク イメージにアクセスする場合に、このオプションを使用します。サポートされる形式は ISO 形式のみです。
   b. [Browse] (参照) をクリックします。
   c. 使用するディスク イメージが含まれるパスを指定して、[Open] (開く) をクリックします。パスが [Image Path] (イメージのパス) フィールドに入力されます。
   d. [接続] をクリックします。
4. ファイル サーバ上のリモート ISO イメージの場合
   a. [Remote Server ISO Image] (リモート サーバの ISO イメージ) オプションを選択します。
   b. ドロップダウン リストから、ホスト名とイメージを選択します。ファイル サーバとイメージ パスは、[File Server Setup] (ファイル サーバのセットアップ) ページを使用して設定できます。[File Server Setup] (ファイル サーバのセットアップ) ページで設定した項目がドロップダウン リストに表示されます。

c. [File Server Username] (ファイル サーバ ユーザ名) - ファイル サーバへのアクセスに必要なユーザ名です。名前には、mydomain/username のようにドメイン名を含めることができます。

d. [File Server Password] (ファイル サーバ パスワード) - ファイル サーバへのアクセスに必要なパスワードです (入力時、フィールドはマスクされます)。

e. [接続] をクリックします。

メディアがターゲット サーバに仮想的にマウントされます。このメディアには、他のドライブとまったく同じようにアクセスすることができます。

注:Linux® ターゲット上のファイルを操作する場合、仮想メディアを使用してコピーしたファイルを表示するには、コピー後に Linux の Sync コマンドを使用します。Sync コマンドを実行するまではファイルを表示できません。

注:Windows 7® オペレーティング システム® を使用している場合、デフォルトでは、ローカル CD/DVD ドライブまたはリモート ISO イメージをマウントしたとき、リムーバブル ディスクは Windows の [マイ コンピュータ] フォルダに表示されません。ローカル CD/DVD ドライブまたはリモート ISO イメージをこのフォルダに表示するには、[ツール] メニューの [フォルダ オプション] をクリックし、[空のドライブは [コンピュータ] フォルダに表示しない] チェック ボックスをオフにします。

注: サードパーティ ソフトウェアの技術的な制限により、IPv6 アドレスを使用して仮想メディア経由でリモート ISO イメージにアクセスすることはできません。

仮想メディア ドライブの切断

▶ 仮想メディア ドライブを切断するには、以下の手順に従います。

- ローカル ドライブの場合は、[Virtual Media] (仮想メディア) の [Disconnect Drive] (ドライブの切断) を選択します。
- CD-ROM、DVD-ROM、ISO イメージの場合は、[Virtual Media] (仮想メディア) の [Disconnect CD-ROM/ISO Image] (CD-ROM/ISO イメージの切断) を選択します。

注:切断コマンドを使用する方法だけでなく、KVM 接続を閉じても仮想メディアが切断されます。

Windows XP 環境での仮想メディア

Virtual KVM Client または Active KVM Client を Windows® XP 環境で実行している場合、CD-ROM 接続、ISO、および ISO イメージを除く仮想メディア タイプにアクセスするには、ユーザに管理者権限が必要です。

Linux 環境での仮想メディア

アクティブ システム パーティション

Linux クライアントからアクティブ システム パーティションをマウントすることはできません。

Linux Ext3/4 ドライブ パーティションは、仮想メディアを接続する前に umount /dev/<device label> でアンマウントしておく必要があります。

ドライブ パーティション

オペレーティング システム間のドライブ パーティションの制限は、以下のとおりです。

- Windows® および Mac の各ターゲットでは Linux 形式のパーティションの読み取りはできない
- Windows および Linux では Mac 形式のパーティションの読み取りはできない
- Linux でサポートされているのは Windows Fat パーティションのみ

root ユーザ権限の要件

Linux クライアントからターゲットに CD ROM をマウントし、その後 CD ROM のマウントを解除する場合は、仮想メディア接続が切断されることがあります。

この問題を回避するには、root ユーザであることが必要です。

Mac 環境での仮想メディア

アクティブ システム パーティション

仮想メディアを使用して、Mac クライアントのアクティブ システム パーティションをマウントすることはできません。

ドライブ パーティション

オペレーティング システム間のドライブ パーティションの制限は、以下のとおりです。

- Windows® および Mac の各ターゲットでは Linux 形式のパーティションの読み取りはできない
- Windows では Mac 形式のパーティションの読み取りはできない
- Windows FAT および NTFS は Mac でサポートされている
- Mac ユーザがターゲットサーバに接続するためには、既にマウントされているデバイスをアンマウントする必要があります。デバイスをアンマウントするには、>diskutil umount /dev/disk1s1 を使用し、再マウントするには、diskutil mount /dev/disk1s1 を使用します。

仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ)

この機能は、仮想メディアを使用してファイル サーバ ISO イメージにアクセスする場合にのみ必要です。Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

注:ファイル サーバには、SMB/CIFS のサポートが必要です。

リモート コンソールの [File Server Setup] (ファイル サーバのセットアップ) ページで、仮想メディアを使用してアクセスするファイル サーバとイメージのパスを指定します。ここで指定されたファイル サーバ ISO イメージは、[Remote Server ISO Image] (リモート サーバの ISO イメージ) で [Hostname] (ホスト名) および [Image] (イメージ) ドロップダウン リスト ([Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックス) の選択肢として表示されます。「*CD-ROM/DVD-ROM/ISO イメージのマウント* 『*277*p. 』」を参照してください。

▶ 仮想メディアとしてアクセスするファイル サーバ ISO イメージを指定するには、以下の手順に従います。

1. リモート コンソールから仮想メディアを選択します。[File Server Setup] (ファイル サーバのセットアップ) ページが開きます。
2. 仮想メディアとしてアクセスするすべてのメディアについて、[Selected] (選択) チェックボックスをオンにします。
3. アクセスするファイル サーバ ISO イメージに関する情報を入力します。
   - [IP Address/Host Name] (IP アドレス/ホスト名) – ファイル サーバのホスト名または IP アドレスです。
   - [Image Path] (イメージのパス) – ISO イメージの場所を表す完全パス名です。たとえば、/sharename0/path0/image0.iso、¥sharename1¥path1¥image1.iso などです。

   注:ホスト名は 232 文字以内で指定してください。

4. [Save] (保存) をクリックします。これで、指定したすべてのメディアが [Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックスで選択できるようになりました。

注:Windows 2003® サーバに接続し、サーバから ISO イメージをロードしようとすると、「Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password」(ポートで仮想メディアのマウントに失敗しました。ファイル サーバに接続できないか、ファイル サーバのユーザ名とパスワードが正しくありません) というエラーが表示される場合があります。このエラーが発生した場合は、[Microsoft ネットワーク サーバー: 通信にデジタル署名を行う] オプションを無効にします。

スマート カード

KX III を使用すると、スマート カード リーダーをターゲット サーバにマウントして、スマート カード認証および関連アプリケーションをサポートできます。

サポートされているスマート カード、スマート カード リーダー、およびシステム要件については、「***スマート カードの最小システム要件、CIM、およびサポートされているスマート カード リーダーとサポートされていないスマート カード リーダー*** 『***281***p. 』」を参照してください。

注:USB スマート カード トークン (eToken NG-OTP) は、リモート クライアントからのみサポートされています。

ローカル コンソールからのスマート カード リーダーのマウントもサポートされます。

Dominion デバイスのヘルプの「***ローカル コンソールのスマート カード アクセス*** 『***307***p. 』」を参照してください。

スマート カードの最小システム要件、CIM、およびサポートされているスマート カード リーダーとサポートされていないスマート カード リーダー

スマート カード リーダーを使用する前に、以下を確認してください。

- ***スマート カードの最小システム要件*** 『***344***p. 』
- ***サポートされているコンピュータ インタフェース モジュール (CIM) の仕様*** 『***338***p. 』
- サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー

スマート カード リーダーへのアクセス時の認証

サーバにリモートでアクセスすると、接続されたスマート カード リーダーを選択し、それをサーバにマウントできます。

スマート カード認証はターゲット サーバで使用されますが、デバイスへのログインには使用されません。したがって、スマート カードの PIN と資格情報を変更するのにデバイス アカウントを更新する必要はありません。

スマート カード使用時の PC 共有モードおよびプライバシー設定

デバイスで PC 共有モードを有効にすると、複数のユーザがターゲット サーバへのアクセスを共有できます。

ただし、スマート カード リーダーがターゲットに接続されている場合は、PC 共有モードの設定にかかわらず、デバイスによってプライバシーが強化されます。

さらに、ターゲット サーバで共有セッションに加わっている場合は、ターゲット サーバへの排他的アクセスが可能になるまでスマート カード リーダーのマウントが無効になります。

スマート カード リーダーの検出

ターゲット サーバとの KVM セッションが確立されると、VKC および AKC で [Smart Card] (スマート カード) メニュー/ボタンを使用できます。

[Smart Card] (スマート カード) ボタンを選択するか、メニューから [Smart Card] (スマート カード) を選択すると、リモート クライアントに接続されているスマート カード リーダーがダイアログ ボックスに表示されます。

このダイアログ ボックスでは、追加のスマート カード リーダーを接続したり、ターゲット サーバに接続されているスマート カード リーダーのリストを更新したり、スマート カード リーダーの接続を解除したりできます。

スマート カードの取り外しと再挿入も行うことができます。この機能を使用して、適切なログイン ダイアログ ボックスを表示するために、カードの取り外しまたは再挿入が必要であるターゲット サーバの OS に通知を送信できます。通知は、他のアクティブな KVM セッションに影響を与えることなく 1 台のターゲット サーバに送信できます。

スマート カード リーダーのマウント

カード リーダーおよびスマート カードをターゲット サーバにマウントすると、サーバはそれらのリーダーやカードが直接接続されているかのように動作します。

スマート カードまたはスマート カード リーダーを取り外すと、ターゲット サーバの OS で設定されているカードの取り外しポリシーに従って、ユーザ セッションがロックされるか、またはユーザがログアウトされます。

KVM セッションが切断されるか、または新しいターゲットに切り替えたために KVM セッションが終了した場合、スマート カード リーダーはターゲット サーバから自動的にマウント解除されます。

▶ VKC または AKC からスマート カード リーダーをマウントするには、以下の手順に従います。

1. [Smart Card] (スマート カード) メニューをクリックし、[Smart Card Reader] (スマート カード リーダー) を選択します。または、ツールバーの [Smart Card] (スマート カード) ボタン をクリックします。
2. [Select Smart Card Reader] (スマート カード リーダーの選択) ダイアログ ボックスでスマート カード リーダーを選択します。
3. [Mount] (マウント) をクリックします。
4. 進行状況を示すダイアログ ボックスが開きます。次回ターゲット サーバに接続したときにスマート カード リーダーを自動的にマウントするには、[Mount selected card reader automatically on connection to targets] (選択したカード リーダーをターゲットへの接続時に自動的にマウントする) チェックボックスをオンにします。[OK] をクリックして、マウント処理を開始します。

スマート カード リーダーの更新

▶ [Select Smart Card Reader] (スマート カード リーダーの選択) ダイアログ ボックスのスマート カード リーダーを更新には、以下の手順に従います。

- 新しいスマート カード リーダーがクライアント PC に接続された場合は、[Refresh List] (リストの更新) をクリックします。

スマート カードの取り外しおよび再挿入の通知の送信

▶ **スマート カードの取り外しおよび再挿入の通知をターゲット サーバに送信するには、以下の手順に従います。**

- 現在マウントされているスマート カード リーダーを選択し、[Remove/Reinsert] (取り外し/再挿入) ボタンをクリックします。

スマート カード リーダーのアンマウント (取り外し)

▶ **スマート カード リーダーのマウントを解除するには、以下の手順に従います。**

- マウントを解除するスマート カード リーダーを選択し、[Unmount] (マウント解除) ボタンをクリックします。

デジタル音声

KX III では、リモート クライアントのデジタル音声再生デバイスおよびキャプチャ デバイスとターゲット サーバ間のエンドツーエンドの双方向デジタル音声接続をサポートしています。

音声デバイスには、USB 接続を介してアクセスされます。

最新のデバイス ファームウェアが必要です。

次のいずれかの CIM を使用する必要があります。

- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

Windows®、Linux®、Mac® の各オペレーティング システムがサポートされています。Virtual KVM Client (VKC) および Active KVM Client (AKC) は、オーディオ デバイスへの接続をサポートしています。

注:音声 CD は、仮想メディアでサポートされていないので、音声機能では使用できません。

音声機能の使用を始める前に、以下のヘルプ セクションに記載されている音声関連情報を確認することを推奨します。

- *サポートされている音声デバイス形式* 『*285*p. 』
- *デュアル ポート ビデオに関する推奨事項* 『*224*p. 』
- *サポートされているマウス モード* 『*224*p. の"*デュアル ビデオ ポート グループでサポートされているマウス モード*"参照 』
- *デュアル ビデオ サポートに必要な CIM* 『*225*p. 』
- 留意事項、*音声* 『*375*p. 』

サポートされている音声デバイス形式

KX III では、ターゲット上の再生デバイスと録音デバイスを 1 台ずつサポートします。サポートされている音声デバイス形式は次のとおりです。

- ステレオ、16 ビット、44.1K
- モノラル、16 ビット、44.1K
- ステレオ、16 ビット、22.05K
- モノラル、16 ビット、22.05K
- ステレオ、16 ビット、11.025K
- モノラル、16 ビット、11.025K

音声の再生とキャプチャに関する推奨事項と要件

音声レベル

- ターゲットの音声レベルを中域に設定します。

  たとえば、Windows® クライアントでは、音声を 50 以下に設定します。

この設定は、クライアントの音声デバイス コントロールではなく、再生またはキャプチャ用の音声デバイスで行う必要があります。

PC 共有モードが有効になっている場合の音声接続に関する推奨事項

PC 共有モードでの動作中に音声機能を使用している場合は、さらに音声デバイスがターゲットに接続されると、音声の再生やキャプチャが中断されます。

たとえば、ユーザ A がターゲット 1 に再生デバイスを接続して音声再生アプリケーションを実行し、ユーザ B が同じターゲットにキャプチャデ バイスを接続するとします。この場合、ユーザ A の再生セッションは中断されるので、音声アプリケーションを再起動する必要があります。

この中断が発生する理由は、新しいデバイス設定で USB デバイスを再列挙する必要があるためです。

ターゲットで新しいデバイスのドライバをインストールする場合は、少し時間がかかることがあります。

音声アプリケーションは、再生の完全な停止、次のトラックへの移動、または再生の続行となる可能性があります。

正確な動作は、音声アプリケーションで切断/再接続イベントがどのように処理されるかによって異なります。

帯域幅要件

次の表は、選択した各形式で音声を転送する場合の音声再生およびキャプチャの帯域幅要件の詳細です。

音声形式	ネットワーク帯域幅要件
44.1 KHz、16 ビット ステレオ	176 kbps
44.1 KHz、16 ビット モノラル	88.2 kbps
2.05 KHz、16 ビット ステレオ	88.2 kbps
22.05 KHz、16 ビット モノラル	44.1 kbps
11.025 KHz、16 ビット ステレオ	44.1 kbps
11.025 KHz、16 ビット モノラル	音声 22.05 kbps

実際に、音声デバイスをターゲットに接続するときに使用される帯域幅は、ターゲットで音声アプリケーションを開いたり使用したりする際に消費されるキーボード データやビデオ データがあるため、広くなっています。

一般的には、再生およびキャプチャを実行する前に、1.5 MB 以上の接続を維持していることを推奨します。

ただし、ターゲット画面の解像度を高くして高品質なビデオ コンテンツをフル カラー接続すると、さらに多くの帯域幅を消費するため、音声の品質が大幅に劣化します。

品質の低下を軽減できるように、帯域幅が狭い場合にビデオが音声品質に与える影響を軽減するための推奨のクライアント設定は数多くあります。

- 音声の再生を低品質の形式で接続します。帯域幅を消費するビデオによる影響は、44k よりも 11k で接続した方が大幅に減少します。
- [Connection Properties] (接続プロパティ) で、接続速度を、クライアントからサーバへの接続に最適な値に設定します。
- [Connection Properties] (接続プロパティ) で、色深度をできる限り低い値に設定します。色深度を 8 ビット カラーにすると、消費される帯域幅が大幅に減少します。
- [Smoothing] (スムージング) を [High] (高) に設定します。これにより、表示されるビデオ ノイズが減少し、ターゲット ビデオの画質が向上します。
- [Video] (ビデオ) 設定で、[Noise Filter] (ノイズ フィルタ) を最も高い設定 7 (最高値) にすると、ターゲットの画面変更に使用される帯域幅が小さくなります。

音声設定の保存

音声デバイス設定は、KX III デバイス単位で適用されます。

KX III の音声デバイス設定が指定され、保存されたら、同じ設定がそのデバイスに適用されます。

たとえば、ステレオ、16 ビット、44.1K の形式を使用するように Windows® 音声デバイスを設定できます。

さまざまなターゲットに接続してその Windows 音声デバイスを使用すると、各ターゲット サーバにはステレオ、16 ビット、44.1K の形式が適用されます。

再生デバイスおよび録音デバイスの両方について、デバイスに適用されるデバイス タイプ、デバイス形式、およびバッファ設定が保存されます。

音声デバイスの接続方法および設定方法については、「***デジタル音声デバイスの接続および切断*** 『*289*p. 』」を参照し、音声デバイスのバッファ設定については、「キャプチャ/再生バッファ サイズの調整 (音声設定)」を参照してください。

複数のユーザがターゲット上の同じ音声デバイスに同時にアクセスできるように、PC 共有モードおよび VM 共有モードでの動作中に音声機能を使用している場合は、セッションを開始するユーザの音声デバイス設定が、セッションに参加するすべてのユーザに適用されます。

したがって、ユーザが音声セッションに参加する場合は、ターゲット マシンの設定が使用されます。「***単一のリモート クライアントから複数のターゲットへの接続*** 『*288*p. 』」を参照してください。

単一のリモート クライアントから複数のターゲットへの接続

単一のリモート クライアントから同時に最大 4 つのターゲット サーバの音声デバイスに接続します。

音声デバイスの接続方法については、「***デジタル音声デバイスの接続および切断*** 『*289*p. 』」を参照してください。

スピーカー アイコン がクライアント ウィンドウの下部のステータス バーに表示されます。音声が使用されていない場合、このアイコンはグレーで表示されます。スピーカー アイコンとマイク アイコン がステータス バーに表示されている場合は、セッションがキャプチャされ、ストリーム配信されます。

注:音声セッションが進行中の場合は、必ずセッションをアクティブなままにするか、KX III のアイドル状態のタイムアウト時間を変更して音声セッションがタイムアウトにならないようにしてください。

オペレーティング システムの音声再生サポート

次の表で、オペレーティング システムごとに音声再生/キャプチャが機能する Raritan クライアントを確認できます。

オペレーティング システム	音声再生およびキャプチャをサポートしているクライアント
Windows®	• Active KVM Client (AKC) • Virtual KVM Client (VKC)
Linux®	• Virtual KVM Client (VKC)
Mac®	• Virtual KVM Client (VKC)

デジタル音声デバイスの接続および切断

音声デバイス設定は、KX III デバイス単位で適用されます。

KX III の音声デバイス設定が指定され、保存されたら、同じ設定がそのデバイスに適用されます。

詳細については、「*音声設定の保存* 『288p. 』」を参照してください。

注:PC 共有モードおよび VM 共有モードでの動作中に音声機能を使用している場合、重要な情報については、「**音声の再生とキャプチャに関する推奨事項と要件** 『285p. 』」*を参照してください。*「**単一のリモート クライアントから複数のターゲットへの接続** 『288p. 』」*も参照してください。*

デジタル音声デバイスの接続

▶ **音声デバイスに接続するには、以下の手順に従います。**

1. 音声デバイスをリモート クライアント PC に接続してから、 KX III とのブラウザ接続を起動します。
2. [Port Access] (ポート アクセス) ページでターゲットに接続します。
3. 接続できたら、ツールバーの [Audio] (音声) ボタン をクリックします。

   [Connect Audio Device] (音声デバイスに接続) ダイアログ ボックスが表示されます。リモート クライアント PC に接続されている利用可能な音声デバイスの一覧が表示されます。

   注:リモート クライアント PC に接続されている利用可能な音声デバイスがない場合、[Audio] (音声) アイコンはグレーで表示されます。.

4. 再生デバイスを接続する場合は、[Connect Playback Device] (再生デバイスを接続) をオンにします。
5. 接続するデバイスをドロップダウン リストから選択します。
6. 再生デバイスの音声形式を [Format:] (形式:) ドロップダウン リストから選択します。

注:使用する形式は、利用可能なネットワーク帯域幅に基づいて選択します。サンプリング レートが低い形式であるほど、消費する帯域幅は少なくなり、ネットワークの輻輳を許容できます。

---

7. 録音デバイスを接続する場合は、[Connect Recording Device] (録音デバイスを接続) をオンにします。

注:[Connect Recording Device] (録音デバイスを接続) ドロップダウンに表示されるデバイス名は、Java クライアント向けに 30 文字に切り捨てられます。

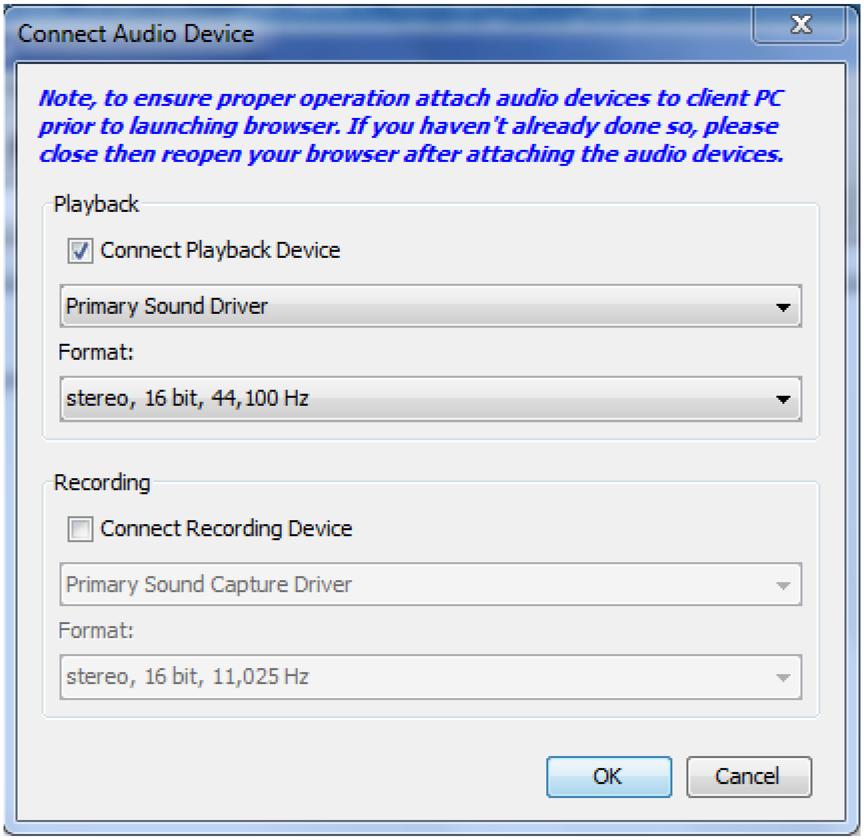
---

8. 接続するデバイスをドロップダウン リストから選択します。
9. 録音デバイスの音声形式を [Format:] (形式:) ドロップダウン リストから選択します。
10. [OK] をクリックします。音声接続が確立されると、確認メッセージが表示されます。[OK] をクリックします。

    音声接続が確立されない場合は、エラー メッセージが表示されます。

    音声接続が確立されると、[Audio] (音声) メニューが [Disconnect Audio] (音声の切断) に変わります。さらに、音声デバイス用の設定は保存され、音声デバイスに適用されます。

スピーカー アイコン がクライアント ウィンドウの下部のステータス バーに表示されます。音声が使用されていない場合、このアイコンはグレーで表示されます。スピーカー アイコンとマイク アイコン がステータス バーに表示されている場合は、セッションがキャプチャされ、ストリーム配信されます。



音声デバイスの切断

▶ 音声デバイスを切断するには、以下の手順に従います。

- ツールバーの［Audio］(音声) アイコン をクリックし、切断を確認するダイアログ ボックスが開かれたら［OK］をクリックします。確認メッセージが表示されます。[OK］をクリックします。

キャプチャ/再生バッファ サイズの調整 (音声設定)

音声デバイスが接続されたら、必要に応じてキャプチャ/再生バッファ サイズを調整できます。

この機能は、音声の品質を管理する場合に役に立ちます。音声の品質は、帯域幅の制限やネットワーク使用量の急増による影響を受けることがあります。

バッファ サイズを増やすと、音声の品質は改善されますが、配信速度が低下することがあります。

有効な最大バッファ サイズは 400 ミリ秒であり、それより大きくすると、音声品質が大幅に低下します。

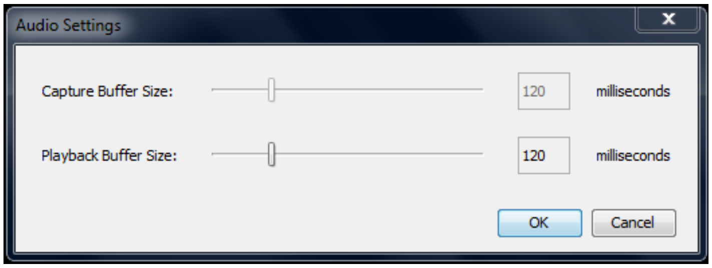
バッファ サイズは、音声セッション中も含めて、必要なときにいつでも調整できます。

音声設定は、VKC または AKC で設定されます。

音声設定の調整

▶ 音声設定を調整するには、以下の手順に従います。

1. [Audio] (音声) メニューから [Audio Settings] (音声設定) を選択します。[Audio Settings] (音声設定) ダイアログ ボックスが開きます。
2. 必要に応じてキャプチャや再生のバッファ サイズを調整します。[OK] をクリックします。



バージョン情報 - Virtual KVM Client

このメニュー コマンドを選択すると、Virtual KVM Client のバージョン情報が表示されます。このバージョン情報は、ラリタン テクニカル サポートを利用するときに必要になります。

▶ バージョン情報を調べるには、以下の手順に従います。

1. [Help] (ヘルプ) の [About Raritan Virtual KVM Client] (バージョン情報) を選択します。

2. 後でサポート時にアクセスできるように、[Copy to Clipboard] (クリップボードにコピー) ボタンを使用して、ダイアログ ボックスに含まれている情報をクリップボード ファイルにコピーします (必要な場合)。

Ch 6　Active KVM Client (AKC) ヘルプ

この章の内容

概要 294
ターゲット サーバへの接続 294
AKC でサポートされている Microsoft .Net Framework 295
AKC でサポートされているオペレーティング システム 295
AKC でサポートされているブラウザ 296
AKC を使用するため前提条件 296

概要

Active KVM Client (AKC) は、Microsoft Windows .NET® 技術に基づいています。

これにより、Raritan の Virtual KVM Client (VKC) の実行に必要な Java® Runtime Environment (JRE) を使用しなくても Windows 環境でクライアントを実行できます。.

AKC は CC-SG とも連動します。

AKC は、以下を除いて VKC と同じ機能を備えています。

- AKC で作成されたキーボード マクロは、VKC では使用不可
- ダイレクト ポート アクセス設定 (「URL を経由したダイレクト ポート アクセスの有効化」を参照)
- AKC サーバ証明書検証設定 (「*AKC を使用するための前提条件*『*296*p. の"*AKC を使用するため前提条件*"参照 』」を参照)
- AKC ではお気に入りが自動的にロードされ、VKC ではロードされない。「お気に入りの管理」を参照

各機能の使用法の詳細については、「*Virtual KVM Client (VKC) ヘルプ*『*242*p. 』」を参照してください。

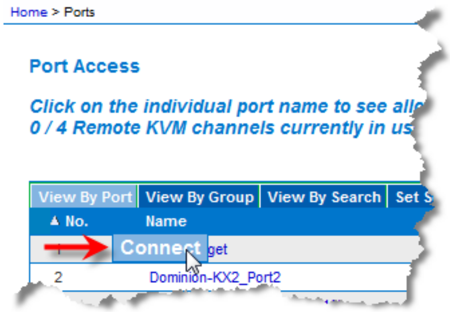
ターゲット サーバへの接続

KX III リモート コンソールにログインしたら、Virtual KVM Client (VKC) または Active KVM Client (AKC) 経由でターゲット サーバにアクセスします。

▶ **利用可能なターゲット サーバまたはデュアル モニタ ターゲット サーバに接続するには、以下の手順に従います。**

1. [Port Access] (ポート アクセス) ページで、接続するターゲット サーバのポート名をクリックします。[Port Action] (ポート アクション) メニューが開きます。

2. ［接続］をクリックします。



使用可能な他のメニュー オプションの詳細については、「*[Port Action] (ポート アクション) メニュー*『*20*p. 』」を参照してください。

AKC でサポートされている Microsoft .Net Framework

Active KVM Client (AKC) には、Windows .NET® バージョン 3.5、4.0、または 4.5 が必要です。AKC は、インストールされている 3.5 および 4.0 の両方と連動します。

AKC でサポートされているオペレーティング システム

Internet Explorer® から起動すると、Active KVM Client (AKC) から KX III を介してターゲット サーバにアクセスできます。

AKC は、以下のプラットフォームに対応しています。

- Windows XP® オペレーティング システム
- Windows Vista® (64 ビット版も可)
- Windows 7® (64 ビット版も可)
- Windows 8® (64 ビット版も可)

注:WINDOWS PC FIPS を有効にし、かつ、AKC とスマート カードを使用してターゲットにアクセスする場合、Windows 7 を使用する必要があります。

AKC を実行するには .NET が必要になるため、.NET がインストールされていない場合、またはサポートされていないバージョンの .NET がインストールされている場合は、.NET バージョンの確認を指示するメッセージが表示されます。

注:Windows XP® オペレーティング システムのユーザは、AKC を起動する前に、基盤となる .NET 3.5 または 4.0 がインストールされているか確認することをお勧めします。.NET バージョンが機能していることを確認できない場合は、.NET バージョンの確認を求めるデフォルトのメッセージが表示される代わりにファイルをダ　ウンロードするよう求められる場合があります。

AKC でサポートされているブラウザ

- Internet Explorer® 8 (以降)

  Internet Explorer 8 (以降) ではないブラウザから AKC を開こうとすると、ブラウザの確認と Internet Explorer への切り替えを指示するエラー メッセージが表示されます。

AKC を使用するため前提条件

Cookie を許可

アクセスするデバイスの IP アドレスからの Cookie が現在ブロックされていないことを確認します。

"信頼済みサイト ゾーン" に KX III IP アドレスを追加

Windows Vista®、Windows® 7、および Windows 2008 Server のユーザは、アクセス対象のデバイスの IP アドレスが、ブラウザの信頼済みサイト ゾーンに追加されていることを確認する必要があります。

"保護モード" を無効化

Windows Vista®、Windows® 7、および Windows 2008 Server のユーザは、KX III にアクセスするときに、保護モードが有効になっていないことを確認する必要があります。

AKC ダウンロード サーバ証明書の検証を有効にする

デバイス (または CC-SG) の管理者が [Enable AKC Download Server Certificate Validation] (AKC ダウンロード サーバ証明書の検証を有効にする) オプションを有効にした場合は、以下の手順に従います。

- 管理者は、有効な証明書をデバイスにアップロードするか、自己署名証明書をデバイスで生成する必要があります。証明書で有効なホストが指定されている必要があります。
- 各ユーザは、CA 証明書 (または自己署名証明書のコピー) をブラウザの信頼されたルート証明機関ストアに追加する必要があります。

CC-SG 管理クライアントから Active KVM Client を起動する場合は、JRE™ 1.7.x (以降) が必要です。

Ch 7 KX III ローカル コンソール - KX III エンド ユーザ ヘルプ

この章の内容

概要 297
ターゲット サーバにアクセスする 297
ローカル コンソールの画面解像度 298
ユーザが同時接続可能 298
ホット キーと接続キー 299
ポートのスキャン - ローカル コンソール 302
ローカル コンソールのスマート カード アクセス 307
ローカル コンソールの USB プロファイル オプション 308
KX III ローカル コンソール ファクトリ リセット 309
デバイスのリセット ボタンによる KX III のリセット 310

概要

ローカル コンソール インタフェースでは、ローカルに KX III にアクセスできます。

このセクションには、ローカル コンソールでエンド ユーザが実行するタスクに関するヘルプが記載されています。

ターゲット サーバにアクセスする

▶ ターゲット サーバにアクセスするには

1. アクセスしたいターゲット サーバのポート名をクリックします。ポート アクション メニューが開きます。
2. ポート アクション メニューの [Connect] (接続) をクリックします。そのターゲット サーバの画面に切り替わります。

ローカル コンソールの画面解像度

KX III ローカル コンソールにモニタを接続すると、KX III でモニタの本来の解像度が検出されます。通常、検出されるのは、モニタでサポートされている最大の解像度です。

モニタの本来の解像度がローカル コンソールでサポートされている場合、KX III では、その解像度が使用されます。

本来の解像度がローカル コンソールでサポートされておらず、それ以外の解像度がモニタおよびローカル コンソールでサポートされていない場合、KX III では、ローカル コンソールに最後に接続したモニタの解像度が使用されます。

たとえば、KX III ローカル コンソールに 1600 x 1200、60Hz の解像度に設定されたモニタを接続するとします。この解像度は、ローカル コンソールでサポートされているので、KX III で使用されます。

次にローカル コンソールに接続するモニタが、サポートされている解像度に設定されていない場合、KX III では、1024 x 768、60Hz の解像度が使用されます。

ローカル コンソールのサポートされている画面解像度については、「*KX III ローカル ポートのサポートされている DVI 解像度* 『*338*p. 』」を参照してください。

さらに、「*ビデオ モードと解像度に関する留意事項* 『*369*p. 』」も確認してください。

ユーザが同時接続可能

KX III ローカル コンソールを使用する場合、接続されている各 KVM ターゲット サーバへの独立したアクセス パスが設定されます。

つまり、KX III ローカル コンソールを使用している最中でも、他ユーザがネットワーク経由で KX III に同時接続できます。また、リモート ユーザが KX III に接続している最中でも、KX III ローカル コンソールを使用してラックからサーバに同時接続できます。

ホット キーと接続キー

KX III ローカル コンソールの画面は、現在アクセスしているターゲット サーバの画面に完全に置き換えられます。ターゲット サーバから切断し、ローカル コンソールの画面に戻るには、ホット キーを使用します。

接続キーは、ターゲット サーバに接続したり、ターゲット サーバを切り替えたりする際に使用します。

ターゲット サーバの画面が表示されているときにホットキーを使用することにより、KX III ローカル コンソールの画面をすばやく開くことができます。

「ローカル コンソールからの KX III ローカル ポートの設定」を参照してください。

KX III ローカル コンソール インタフェースへの切り替え - デフォルトのホット キー

▶ ターゲット サーバの画面から KX III ローカル コンソールの画面に戻るには

- Scroll Lock キーをすばやく 2 回押します。

  ターゲット サーバの画面から KX III ローカル コンソールの画面に切り替わります。

このキー組み合わせを変更するには、[Local Port Settings] (ローカル ポート設定) ページを使用します。オンライン ヘルプの「**ローカル コンソールからの KX III ローカル ポートの設定**」を参照してください。

接続キーの例

標準型サーバの場合	
接続キーを押したときのアクション	**キー組み合わせの例**
KX III ローカル コンソールからポートに接続する	KX III ローカル コンソールからポート 5 に接続するには • 左 Alt キーを押す → 5 キーを押して離す → 左 Alt キーを離す
ポートを切り替える	ポート 5 からポート 11 に切り替えるには • 左 Alt キーを押す → 1 キーを押して離す → 1 キーを押して離す → 左 Alt キーを離す
ターゲット サーバから切断し、KX III	ポート 11 から切断し、KX III ローカル コンソールの画面 (ターゲット サーバに接続する時に

標準型サーバの場合	
接続キーを押したときのアクション	**キー組み合わせの例**
ローカル コンソールの画面に戻る	開いていたページ）に戻るには • Scroll Lock キーをすばやく 2 回押す
ブレード シャーシの場合	
接続キーを押したときのアクション	**キー組み合わせの例**
KX III ローカル コンソールからポートに接続する	ポート 5 のスロット 2 に接続するには • 左 Alt キーを押す →5 キーを押して離す →2 キーを押して離す → 左 Alt キーを離す
ポートを切り替える	ポート 5 のスロット 2 からポート 5 のスロット 11 に切り替えるには • 左 Alt キーを押す →5 キーを押して離す →1 キーを押して離す →1 キーを押して離す → 左 Alt キーを離す
ターゲット サーバから切断し、KX III ローカル コンソールの画面に戻る	ポート 11 のスロット 11 から切断し、KX III ローカル コンソールの画面（ターゲット サーバに接続する時に開いていたページ）に戻るには • Scroll Lock キーをすばやく 2 回押す

Sun サーバへのアクセス時に使用できる特別なキー組み合わせ

ローカル ポートでは、Sun Microsystems™ サーバの特別なキーに対して、次のキー組み合わせが機能します。これらの特別なキー組み合わせは、Sun ターゲット サーバに接続しているときに使用できます。

Sun サーバのキー	ローカル ポートにおけるキー組み合わせ
Again	Ctrl+ Alt +F2
Props	Ctrl+ Alt +F3
Undo	Ctrl+ Alt +F4
Stop A	Break a
Front	Ctrl+ Alt +F5
Copy	Ctrl+ Alt +F6
Open	Ctrl+ Alt +F7
Find	Ctrl+ Alt +F9
Cut	Ctrl+ Alt +F10
Paste	Ctrl+ Alt +F8
Mute	Ctrl+ Alt +F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol −	Ctrl + Alt + KPAD −
Stop	キー組み合わせなし
電力	キー組み合わせなし

ポートのスキャン - ローカル コンソール

ポート スキャン機能を使用して、選択したターゲットを検索し、それをスライド ショーの一部として個々のサムネイルで表示します。

この機能により、スライド ショーの間に表示される各ターゲット サーバを個々に表示できるので、一度に最大 32 のターゲットを監視できます。

ターゲットに接続するか、必要に応じて特定のターゲットをフォーカスします。

スキャン対象は、標準ターゲット、ブレード サーバ、カスケード接続 Dominion デバイス、KVM スイッチの各ポートです。

デュアル ビデオ ポート グループでは、プライマリ ポートはポート スキャンの対象になりますが、リモート クライアントから接続する場合、セカンダリ ポートは対象になりません。両方のポートをローカル ポートからスキャンの対象にすることができます。

任意のターゲット サーバのサムネイルをクリックし、スキャン モードを終了してターゲットに接続するか、ローカル ポートの ConnectKey シーケンスを使用します。

スキャン モードを終了するには、サムネイル表示で [Stop Scan] (スキャンの停止) ボタンをクリックするか、DisconnectKey シーケンス ホットキーを使用します。

注:ポート スキャン機能は、リモート コンソールとローカル コンソールで使用できますが、機能はわずかに異なっています。「ポートのスキャン - リモート コンソール」を参照してください。

ポートのスキャンのスライド ショー - ローカル コンソール

スキャンを開始すると、[Port Scan] (ポート スキャン) ウィンドウが開きます。

ターゲットが見つかるたびに、スライド ショーのサムネイルとして表示されます。

スライド ショーでは、デフォルト間隔の 10 秒ごとに、またはユーザが指定した間隔に従ってターゲットのサムネイルがスクロールされます。

スキャンによってターゲットがスクロールされるときは、スライド ショーでフォーカスされているターゲットがページの中央に表示されます。

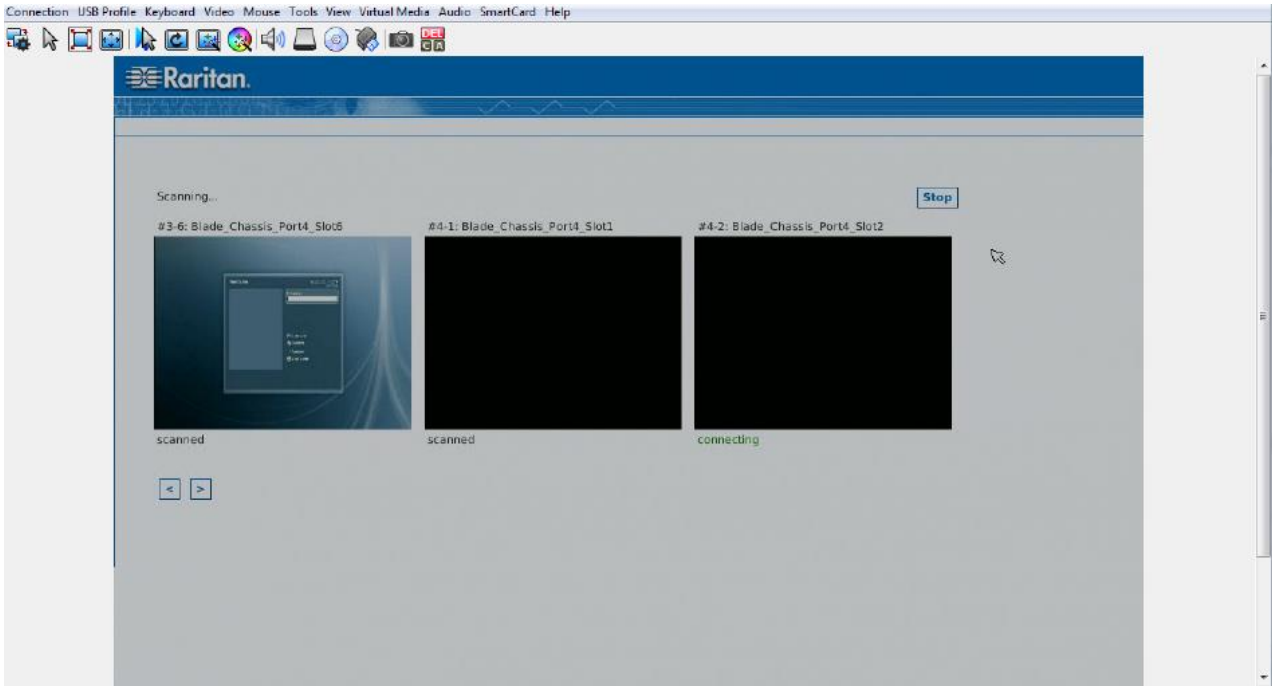
ターゲット名はサムネイルの下とウィンドウ下部のタスクバーに表示されます。

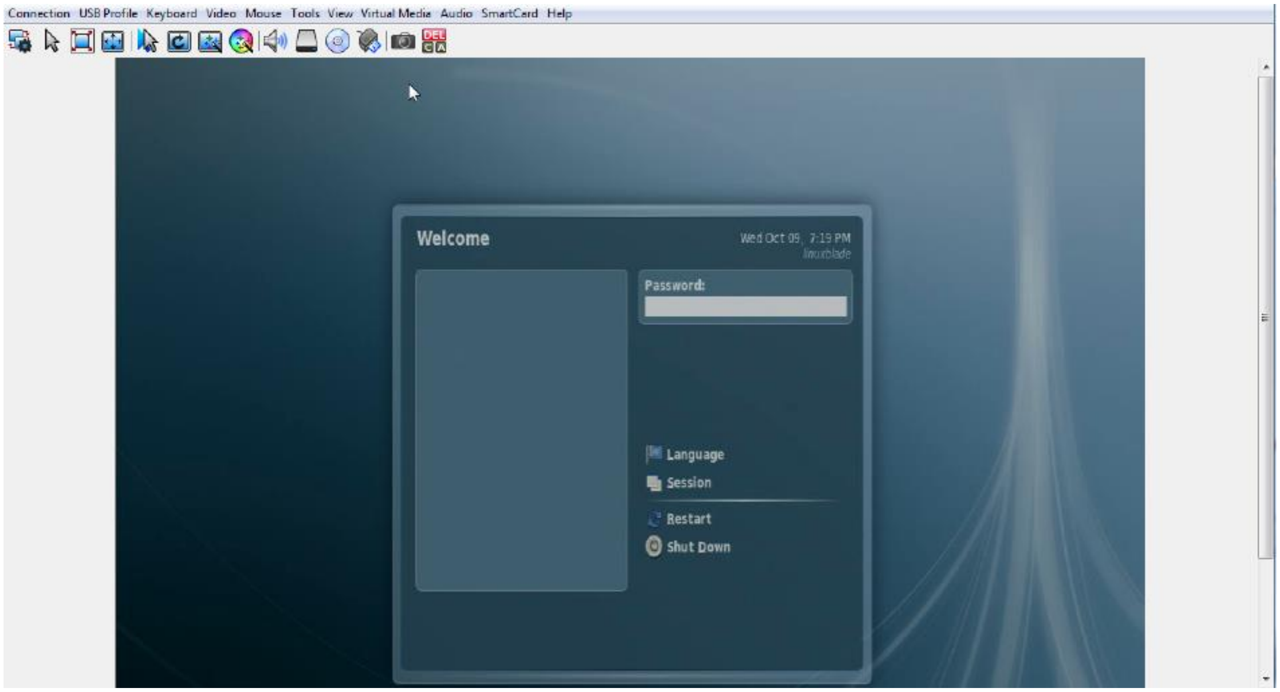
ターゲットがビジーである場合は、ターゲット サーバへのアクセス ページの代わりに空白の画面が表示されます。

[Local Port Settings] (ローカル ポート設定) ページでスライド ショーのサムネイルのローテーション時間およびサムネイル フォーカス間隔を設定します。

「*ローカル コンソール スキャンの設定* 『*305*p. 』」を参照してください。

注:Virtual KVM Client (VKC) または Active KVM Client (AKC) からリモート コンソールのスキャン設定を指定します。「VKC および AKC でのポート スキャンの設定 『268*p.* 』」*を参照してください。*



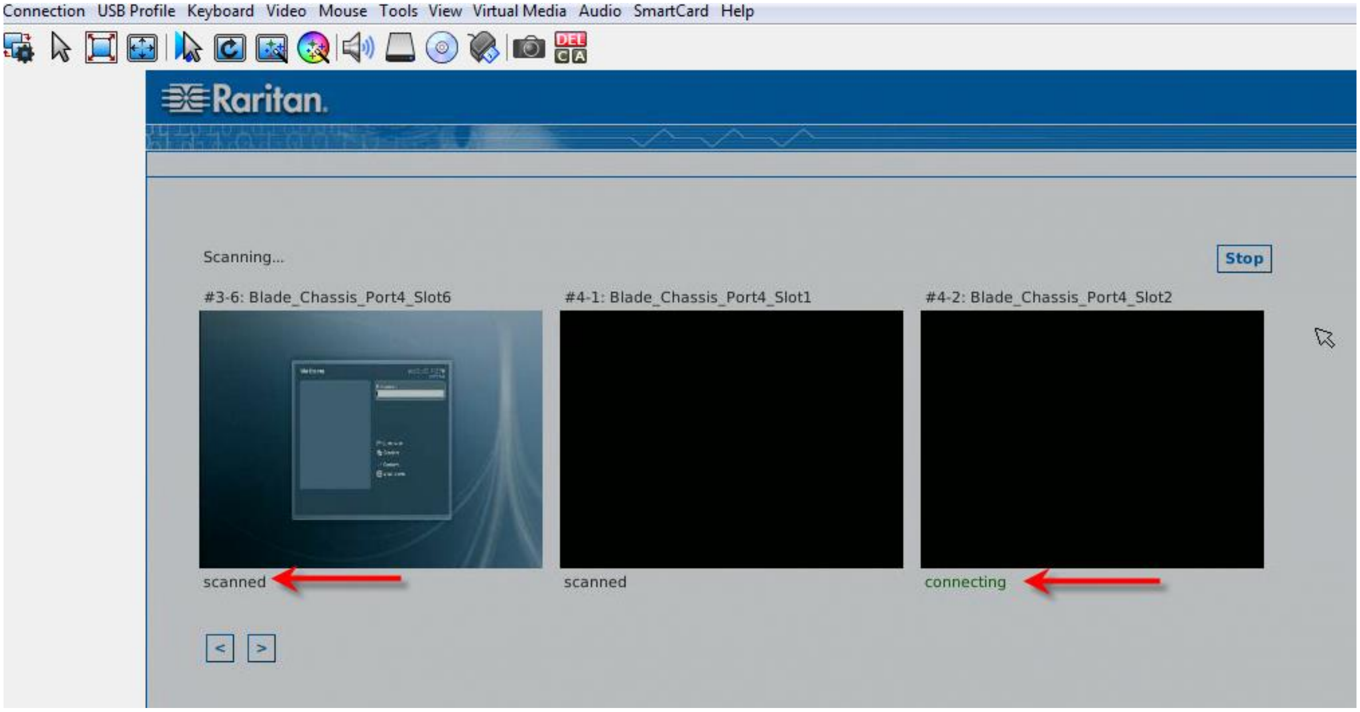

Connection USB Profile Keyboard Video Mouse Tools View Virtual Media Audio SmartCard Help
Welcome
Password:
Language
Session
Restart
Shut Down

ポート スキャン中のターゲット ステータス インジケータ - ローカル コンソール

ローカル コンソールのサムネイル表示では、各ターゲットがスライド ショー ビューでフォーカスされるまで、そのステータスがページのサムネイルの下に示されます。

各ターゲットのスキャン ステータスは、次のように表示されます。

- not scanned (未スキャン)
- connecting (接続中)
- scanned (スキャン済み)
- skipped (スキップ)



ローカル コンソール スキャンの設定

ローカル コンソールのポート スキャン オプションを設定するには、以下の手順に従います。

注:Virtual KVM Client (VKC) または Active KVM Client (AKC) からリモート コンソールのスキャン設定を指定します。「**VKC および AKC でのポート スキャンの設定** 『268p. 』」*を参照してください。*

▶ **ローカル コンソールのスキャン ポートを設定するには、以下の手順に従います。**

1. ローカル コンソールで、[Device Settings] (デバイス設定) を選択します。

2. [Local Port Settings] (ローカル ポート設定) セクションで、[Local Port Scan Mode] (ローカル ポート スキャン モード) を選択します。
3. 必要に応じて表示間隔を変更します。
   - [Display Interval] (表示間隔) - スキャン表示間隔を変更します。
   - [Interval Between Ports] (ポート間の間隔) - スキャン中にさまざまなポートを切り替える間隔を変更します。

ターゲットのスキャン - ローカル コンソール

▶ ターゲットをスキャンするには、以下の手順に従います。

1. [Port Access] (ポート アクセス) ページの [Set Scan] (スキャン設定) タブをクリックします。
2. 各ターゲットの横にあるチェックボックスをオンにしてスキャン対象に含めるターゲットを個別に選択するか、ターゲット列の上部にあるチェックボックスをオンにしてすべてのターゲットを選択します。
3. アップ ステータスのターゲットだけをスキャンに含める場合は、[Up Only] (アップのみ) チェックボックスをオンのままにします。アップかダウンかに関係なくすべてのターゲットを含める場合は、このチェックボックスをオフにします。
4. [Scan] (スキャン) をクリックしてスキャンを開始します。

   スキャンされたターゲットは、ページのスライド ショー ビューに表示されます。

ローカル コンソールのスマート カード アクセス

ローカル コンソールでスマート カードを使用してサーバにアクセスするには、KX III に搭載されているいずれかの USB ポートを使用して USB スマート カード リーダーを KX III に接続します。

スマート カード リーダーは、KX III に接続したり KX III から取り外したりすると、KX III によって自動検出されます。

サポートされているスマート カードおよびシステム要件の一覧については、「サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー」および「*スマート カードの最小システム要件* 『*344*p. 』」を参照してください。

カード リーダーおよびスマート カードをターゲット サーバにマウントすると、サーバはそれらのリーダーやカードが直接接続されているかのように動作します。

スマート カードまたはスマート カード リーダーを取り外すと、ターゲット サーバの OS で設定されているカードの取り外しポリシーに従って、ユーザ セッションがロックされるか、またはユーザがログアウトされます。

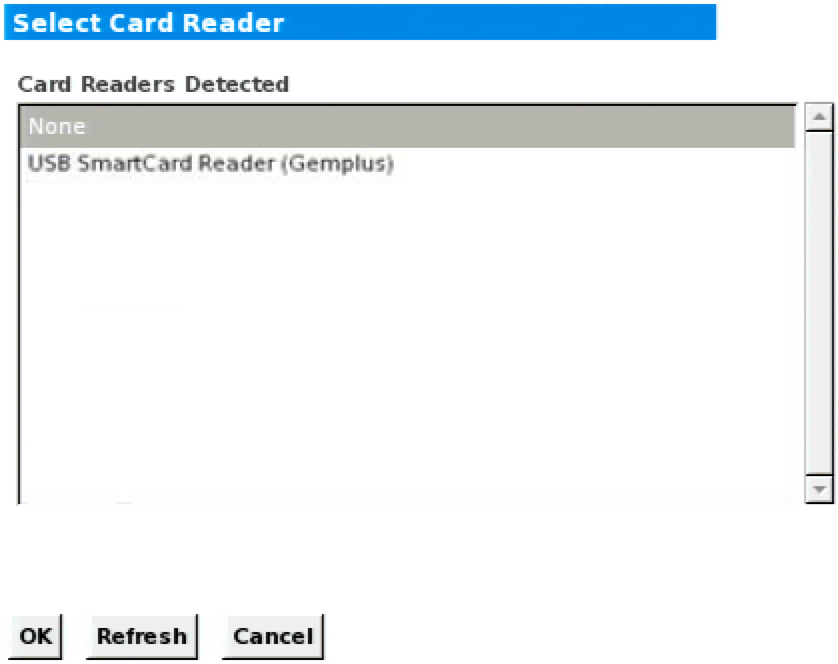
KVM セッションが切断されるか、または新しいターゲットに切り替えたために KVM セッションが終了した場合、スマート カード リーダーはターゲット サーバから自動的にマウント解除されます。

► **KX III ローカル コンソールからスマート カード リーダーをターゲットにマウントするには、以下の手順に従います。**

1. デバイスに搭載されているいずれかの USB ポートを使用して、USB スマート カード リーダーを KX III に接続します。接続すると、スマート カード リーダーは KX III によって検出されます。
2. ローカル コンソールで [Tools] (ツール) をクリックします。
3. [Card Reader Detected] (検出されたカード リーダー) リストからスマート カード リーダーを選択します。スマート カード リーダーをマウントしない場合は、リストから [None] (なし) を選択します。
4. [OK] (OK) をクリックします。スマート カード リーダーを追加すると、操作が正常に完了したことを示すメッセージがページに表示されます。ページの左パネルの [Card Reader] (カード リーダー) に、状態として [Selected] (選択) または [Not Selected] (未選択) が表示されます。

[Card Readers Detected] (検出されたカード リーダー) リストを更新するには、以下の手順に従います。

- 新しいスマート カードがマウントされた場合は、[Refresh] (更新) をクリックします。[Card Readers Detected] (検出されたカード リーダー) リストが更新され、新しく追加されたスマート カード リーダーが表示されます。



ローカル コンソールの USB プロファイル オプション

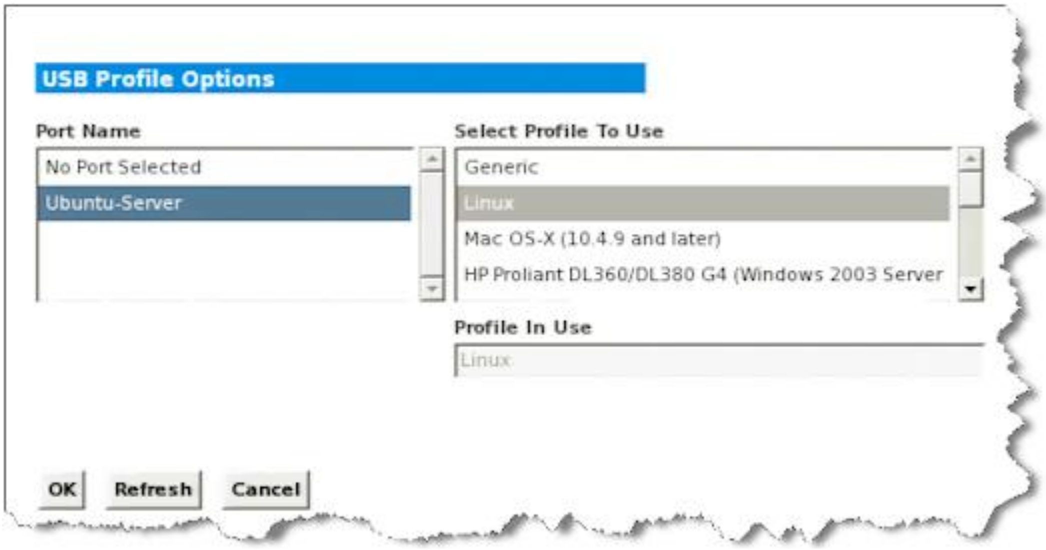
[Tools] (ツール) ページの [USB Profile Options] (USB プロファイル オプション) セクションで、USB プロファイルを選択できます。

プロファイルを適用可能なポートが [Port Name] (ポート名) フィールドに表示されます。ポートを選択すると、そのポートに適用可能なプロファイルが [Select Profile To Use] (使用するプロファイルを選択) フィールドに表示されます。ポートに対して選択したプロファイルは、[Profile In Use] (使用中のプロファイル) フィールドに表示されます。

USB プロファイルをローカル コンソール ポートに適用するには

1. [Port Name] (ポート名) フィールドで、USB プロファイルを適用するポートを選択します。
2. [Select Profile To Use] (使用するプロファイルを選択) フィールドで、そのポートに適用するプロファイルを選択します。

3. [OK] (OK) をクリックします。その USB プロファイルがローカル ポートに適用され、また、[Profile In Use] (使用中のプロファイル) フィールドに表示されます。



KX III ローカル コンソール ファクトリ リセット

注:出荷時設定にリセットする前に、監査ログを保存しておくことを推奨します。

*出荷時設定にリセットされると、監査ログが削除されます。また、リセット イベントは監査ログに記録されません。監査ログの保存手順については、「**監査ログ** 『188p. の"[Audit Log] (監査ログ)"参照 』」を参照してください。*

▶ 出荷時設定にリセットするには

1. [Maintenance] (保守) メニューの [Factory Reset] (出荷時設定にリセット) をクリックします。[Factory Reset] (出荷時設定にリセット) ページが開きます。
2. リセット モードを選択します。選択できるオプションは次のとおりです。
   - [Full Factory Reset] (完全リセット): すべての設定値を削除し、工場出荷時のデフォルト値にリセットします。KX III が CC-SG の管理下にある場合は、CC-SG との関連付けが解除されます。このリセット モードではすべての設定値がリセットされるので、リセットしてもよいかどうかを確認するためのダイアログ ボックスが開きます。

- [Network Parameter Reset] (ネットワーク パラメータ値をリセット): デバイスのネットワーク パラメータ値を出荷時設定にリセットします。パラメータ値を表示するには、[Device Settings] (デバイス設定) の [Network Settings] (ネットワーク設定) をクリックします。

3. [Reset] (リセット) をクリックして続行します。すべてのネットワーク設定値がリセットされるので、リセットしてもよいかどうかを確認するためのダイアログ ボックスが開きます。
4. [OK] をクリックして続行します。リセットが完了すると、KX III が自動再起動します。

デバイスのリセット ボタンによる KX III のリセット

デバイスの背面パネルにリセット ボタンがあります。誤ってリセットされることがないように、ボタンはパネルに埋め込まれています (このボタンを使用するには、先端が尖った道具が必要です)。

リセット ボタンを押したときに実行される処理については、[Encryption & Share] (暗号化および共有) ページで定義します。「暗号化および共有」を参照してください。参照してください。

注:出荷時設定にリセットする前に、監査ログを保存しておくことを推奨します。

*出荷時設定にリセットされると、監査ログが削除されます。また、リセット イベントは監査ログに記録されません。監査ログの保存手順については、**「**監査ログ** 『**188**p. の"**[Audit Log] (監査ログ)**"参照 』」を参照してください。*

▶ デバイスをリセットするには、以下の手順に従います。

1. KX III の電源を切ります。
2. 先端の尖った道具を使用してリセット ボタンを押し続けます。
3. リセット ボタンを押したまま、KX III の電源を入れ直します。

4. リセット ボタンを 10 秒間押したままにします。

Ap A　KX III と Cat5 Reach DVI の接続 - 拡張ローカル ポート機能の提供

この章の内容

概要 312
Cat5 Reach DVI の概要 312
KX III と Cat5 Reach DVI の接続 313

概要

拡張ローカル ポートは、KX III を収容しているラックを越えて、たとえば別の KVM スイッチまでローカル ポートの接続距離を延長します。

接続距離を延長するには、リモート コンソールまたは他のデバイスに接続されている Raritan Cat5 Reach DVI トランスミッタやレシーバと連動するように KX III を設定します。

Cat5 Reach DVI に接続すると、KX III は、最大 152 m (500 フィート) 離すことができます。

Ethernet スイッチをデイジーチェーン接続して KX III を Cat5 Reach DVI に接続すると、KX III の接続距離を 914 m (3000 フィート) まで延長できます。

Cat5 Reach DVI の概要

Cat5 Reach DVI の詳細については、*Raritan サポート ページ http://www.raritan.com/support* で利用可能な Cat5 Reach DVI オンライン ヘルプを参照してください。

Cat5 Reach DVI に関する追加情報や購入に関する情報については、*Raritan にお問い合わせください* 『*http://www.raritan.com/contact-us/*参照 』。

KX III と Cat5 Reach DVI の接続

注:図中の画像は、KX III を特定するものではありませんが、接続は正確です。

このセクションでは、KVM スイッチを使用する 3 つのシナリオを説明します。

- KVM スイッチとそのローカル コンソールの間に Cat5 Reach DVI を接続します。
- 2 つの KVM スイッチの間に Cat5 Reach DVI を接続します。
- コンピュータ/サーバと KVM スイッチの間に Cat5 Reach DVI を接続します。

接続する前にすべてのデバイスの電源をオフにします。

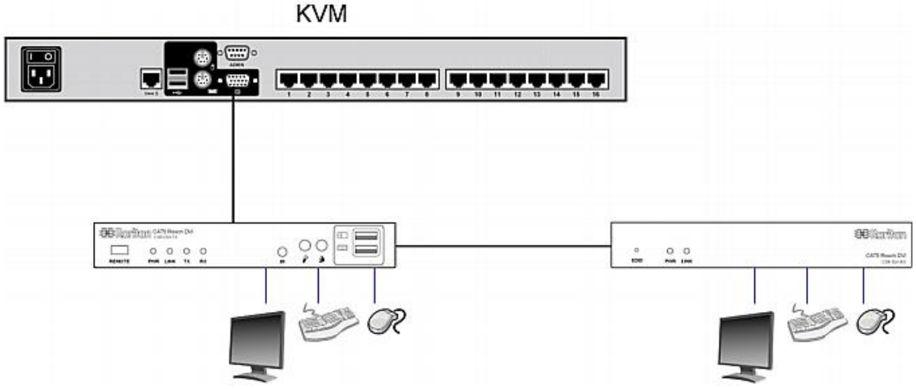
ローカル コンソールおよびリモート コンソールのセットアップの詳細については、**Cat5 Reach DVI ヘルプ**の「**Connecting a Keyboard/Mouse/Video Source (キーボード/マウス/ビデオ ソースの接続)**」を参照してください。

▶ KX III と Cat5 Reach DVI を接続するには、以下の手順に従います。

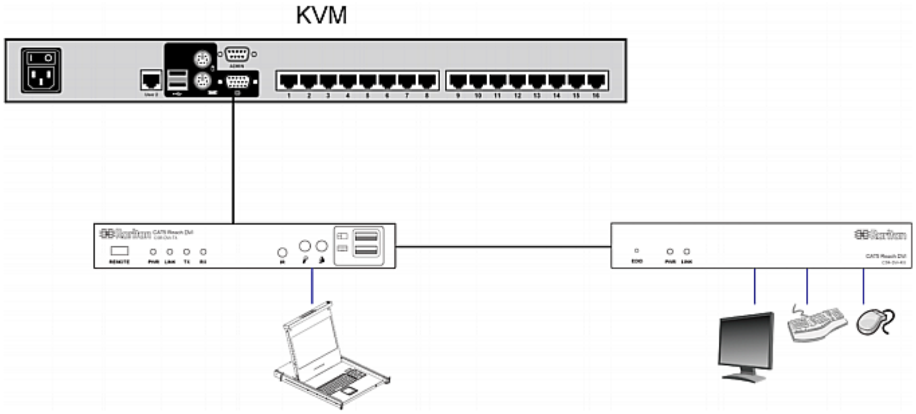
1. セットアップがまだの場合は、ローカル コンソールおよびリモート コンソールを、それぞれ Cat5 Reach DVI トランスミッタおよびレシーバと共にセットアップします。

   詳細については、**Cat5 Reach DVI ヘルプ**の「**Basic Installation (基本インストール)**」を参照してください。
2. Cat5e/6 ケーブルを使用してトランスミッタおよびレシーバを接続します。
3. トランスミッタおよびレシーバをそれぞれ適切な電源に接続します。
4. KVM スイッチのローカル コンソール ポートをトランスミッタに接続します。
   a. Raritan が提供する DVI ケーブルの片側をトランスミッタの DVI-I IN ポートに接続し、反対側を KVM スイッチのビデオ ポートに接続します。
   b. Raritan が提供する USB ケーブルの USB-B コネクタをトランスミッタの USB-B ポートに接続し、反対側を KVM スイッチのローカル USB-A ポートに接続します。

5. KVM スイッチの電源をオンにします。



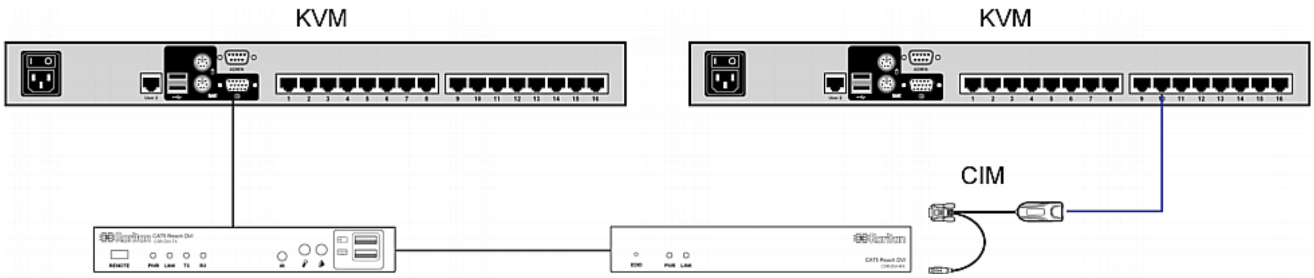
ヒント: ローカルまたはリモート コンソールには、キーボード、マウス、およびモニタのセットではなく、KVM ドロワーを装備できます。下の図を参照してください。



▶ 2 つのカスケード接続 KVM スイッチ間の距離を延ばすには、以下の手順に従います。

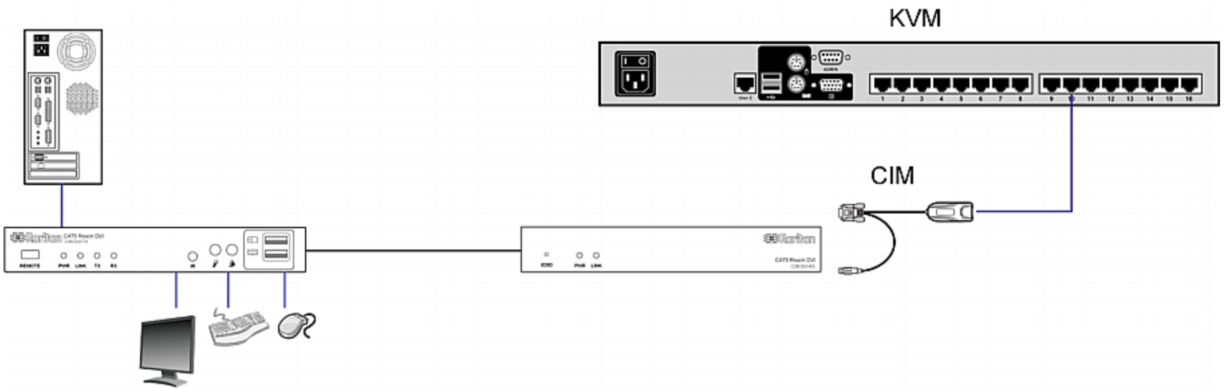
1. レシーバを KVM スイッチに接続して、リモート コンソールをセットアップします。
   a. USB CIM をレシーバに接続します。
   b. この USB CIM を Cat5 ケーブルで KVM スイッチの任意のチャネル ポートに接続します。
2. Cat5e/6 ケーブルを使用してトランスミッタおよびレシーバを接続します。
3. トランスミッタおよびレシーバをそれぞれ適切な電源に接続します。
4. KVM スイッチをトランスミッタに接続します。

5. 両方の KVM スイッチの電源をオンにします。



コンピュータと KVM スイッチの間の距離を延ばすには、以下の手順に従います。

1. オプションのローカルコンソールとトランスミッタをセットアップします。
2. レシーバを KVM スイッチに接続して、リモート コンソールをセットアップします。
3. Cat5e/6 ケーブルを使用してトランスミッタおよびレシーバを接続します。
4. トランスミッタおよびレシーバをそれぞれ適切な電源に接続します。
5. コンピュータをトランスミッタに接続します。
6. コンピュータの電源をオンにします。



Ap B　KX III から Paragon II へのアクセス

この章の内容

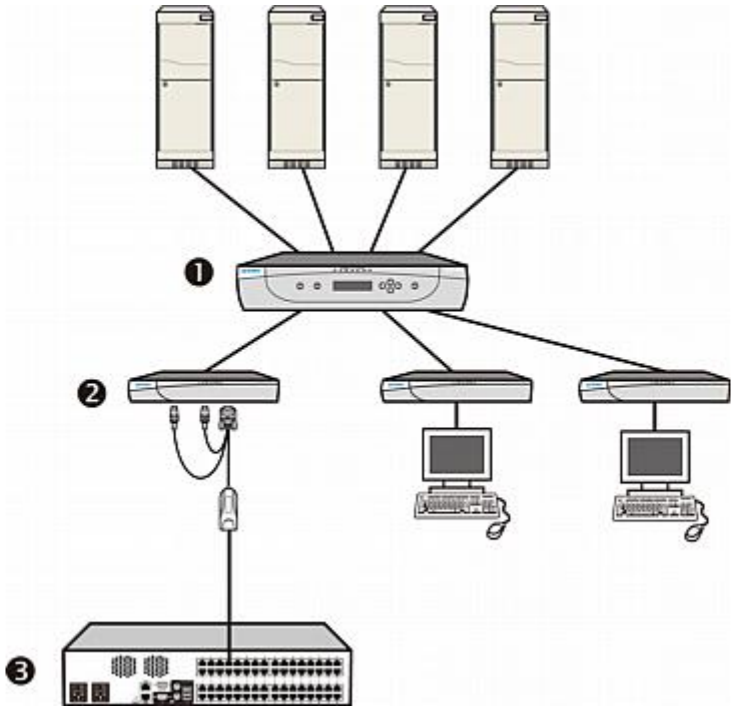
概要 316
サポートされている Paragon II CIMS および設定 317
KX III への Paragon II の接続.. 322

概要

CC-SG から Paragon II にアクセスできるように、Paragon II システムを CC-SG で管理されている KX III デバイスに接続します。

この図は、KX III の統合構成を示しています。

注:画像は、例にすぎず、お使いのデバイスと異なる場合があります。



❶	Paragon II のスイッチ、サーバ、およびユーザ ステーションが接続されている Paragon II システム
❷	DCIM-USB G2 を搭載したユーザ ステーション
❸	KX III

KX III または CC-SG から Paragon II システムにアクセスすると(KX III が CC-SG の管理下にある場合)、Paragon II OSUI ログイン画面が表示されます。

この統合では、現在の Paragon II ファームウェアで実装されている OSUI 機能または現在の KX III ファームウェアで実装されている KX III 機能(仮想メディア機能を除く)を実行できます。

KX III を介して Paragon II OSUI にアクセスする場合は、手動でマウスを同期しないでください。OSUI 画面ではマウスは不要であり、マウスを同期すると、キーボードの応答が数秒遅れます。

詳細については、「*サポートされている Paragon II CIMS および設定*『*317*p. 』」を参照してください。

サポートされている **Paragon II CIMS** および設定

KX III では P2CIM-APS2DUAL CIM および P2CIM-AUSBDUAL CIM がサポートされています。これらの CIM を使用した場合、RJ45 で 2 台の異なる KVM スイッチに接続できます。

これらの CIM がサポートされているので、KVM スイッチのいずれかに障害が発生した場合に備えて、ターゲットにアクセスするための 2 つ目の経路を確保できます。

Paragon CIM	サポートされるもの	サポートされないもの
P2CIM-APS2DUAL	• IBM® PS/2 型のキーボード ポートとマウス ポートを備えたサーバ • 自動スキュー補正 (CIM が Paragon II に接続されているが、KX III に接続されていない場合) • インテリジェント マウス モード • 標準マウス モード	• 仮想メディア • スマート カード • ずれないマウス モード • ブレード シャーシとの併用 • KVM のカスケード接続構成

Paragon CIM	サポートされるもの	サポートされないもの
P2CIM-AUSBDUAL	• USB 型または Sun™ USB 型のキーボード ポートとマウス ポートを備えたサーバ • 自動スキュー補正 (CIM が Paragon II に接続されているが、KX III に接続されていない場合) • インテリジェント マウス モード • 標準マウス モード	• 仮想メディア • スマート カード • ずれないマウス モード • ブレード シャーシとの併用 • KVM のカスケード接続構成

KX III - KX III 構成の Paragon CIM に関するガイドライン

KX III - KX III 構成で Paragon CIM を使用する場合は、次に示すシステム構成ガイドラインに従ってください。

同時アクセス

両方の KX III KVM スイッチで、ターゲットへの同時アクセスに対して同じポリシーを設定する必要があります。つまり、どちらも [PC-Share] (PC 共有) にするか、どちらも [Private] (プライベート) に設定します。

ターゲットへのプライベート アクセスが必要な場合は、どちらの KVM スイッチもそれに応じて構成する必要があります。

- [Security] (セキュリティ)、[Security Settings] (セキュリティ設定)、[Encryption & Share] (暗号化および共有) を選択し、[PC Share Mode] (PC 共有モード) を [Private] (プライベート) に設定します。

これにより、すべてのユーザ グループおよびすべてのターゲットにおいて、ターゲットへの同時アクセスはできなくなります。

KX III では、ターゲットへの同時アクセスをより高い粒度で、ユーザ グループ単位で制御できます。これは、ユーザ グループの PC 共有権限を設定することで行われます。ただし、これが適用されるのは KX III の範囲内のみです。P2CIM-APS2DUAL または P2CIM-AUSBDUAL を KX III と組み合わせて使用する際にプライバシーを保証する必要がある場合、ユーザ グループに対する PC 共有権限を使用しないでください。

CIM 名の更新

P2CIM-APS2 および P2CIM-AUSB の名前は CIM のメモリに保持されています。メモリ上には、Paragon CIM の名前 (最大 12 文字) を保持するための領域と、KX III の名前 (最大 32 文字) を保持するための領域の、2 つの領域があります。

Paragon CIM を KX III に初めて接続したとき、CIM の名前がメモリから取得され、KX III によって使用される CIM のメモリ領域に書き込まれます。続いて、KX III から、KX III によって使用されるメモリ領域に対して、CIM 名の照会または更新が行われます。KX III から、Paragon II によって使用されるメモリ領域に対して更新が行われることはありません。

一方の KX III によって CIM 名が更新されると、もう一方の KX III がそのターゲットへの接続を試みるときに、更新後の CIM 名が検出および取得されます。そのときまで、この CIM 名がもう一方の KX III 上で更新されることはありません。

ポートのステータスと可用性

ポートのステータスは、KX III の [Port Access] (ポート アクセス) ページに [Up] (稼動) または [Down] (非稼動) として表示されます。このステータスは最新の情報に更新され、CIM の電源が入っていて KX III のポートに接続されているかどうかが示されます。

ポートの可用性は、KX III の [Port Access] (ポート アクセス) ページに [Idle] (アイドル)、[Busy] (ビジー)、または [Connected] (接続) として表示されます。この可用性情報は、同じ KX III から起動されたターゲットの稼動状況を反映するように更新されます。

もう一方の KX III からそのターゲットに接続している場合は、この KX III から接続が試みられたときに可用性が検査されます。KX III に対して設定されている PC 共有ポリシーに基づいて、アクセスが拒否または許可されます。そのときまで、この可用性情報がもう一方の KX III 上で更新されることはありません。

ターゲットがビジーであるためにアクセスが拒否された場合、通知が表示されます。

CC-SG との連係動作

CC-SG から起動される処理は、管理対象 KX III から通知されるステータス、可用性情報、および CIM 名に基づいて決まります。ターゲットが 2 台の管理対象 KX III に接続されており、これらの KX III が CC-SG に追加されている場合、ノードが 2 つ作成されます。各ノードには固有の oob-kvm インタフェースが関連付けられます。各 KX III の oob-kvm インタフェースで、単一のノードを設定することもできます。

KX III がプライベート モードに設定されている場合、2 つ目の接続が試みられると、"接続できず、アクセスが拒否された" という内容のメッセージがユーザに表示されます。

CC-SG の [Port Profile] (ポート プロファイル) ペインでポート名を変更すると、変更後の名前が管理対象 KX III にプッシュ送信されます。もう一方の KX III の対応するポート名は、そのもう一方の oob-kvm インタフェース経由でターゲットへの接続が試みられるまで、CC-SG 内で更新されません。

KX III - Paragon II 構成に関するガイドライン

P2CIM-APS2DUAL または P2CIM-AUSBDUAL を使用して KX III と Paragon II を接続できます。

同時アクセス

KX III と Paragon II の両方で、ターゲットへの同時アクセスに関して同じポリシーを設定してください。

Paragon II の動作モード	モードの説明	サポート
プライベート	特定のチャネル ポートに接続されているサーバなどのデバイスに、同時に 1 人のユーザだけが排他アクセスできます。	サポートされています。 Paragon II と KX III の両方を [Private] (プライベート) に設定する必要があります。プライベート設定は、ユーザ

Paragon II の動作モード	モードの説明	サポート
		グループごとではなく KX III に対して適用されます。 Paragon II では、赤は "ビジー"、緑は "使用可能" を意味します。
PC 共有	特定のチャネル ポートに接続されているサーバなどのデバイスを、複数のユーザが選択して制御することができます。ただし、キーボードとマウスを制御できるユーザは同時に 1 人だけです。	サポートされています。 ただし、Paragon II で設定される PC 共有アイドル タイムアウトはサポートされていません。両方のユーザが、キーボードとマウスを同時に制御できます。 Paragon II では、緑は "使用可能" を意味します。このことは、別のユーザが既にターゲットにアクセスしている場合にも当てはまります。
パブリック表示	一方のユーザが、特定のチャネル ポートに接続されているサーバなどのデバイスにアクセスしている間、もう一方のユーザは、そのチャネル ポートを選択し、そのデバイスからのビデオ出力を表示することができます。ただし、キーボードとマウスを制御できるのは、最初にアクセスしたユーザだけです。両方のユーザが切断するか、またはキーボードとマウスを取り外すと、この状態が解消されます。	サポートされていません。 Paragon II と KX III を CIM で接続している場合、このモードは使用できません。 Paragon II では、黄色はパブリック表示モードを意味します。

CIM 名の更新

- Paragon II から更新された CIM 名は、Paragon の命名規則に対応する CIM メモリ領域に保持され、この領域から取得されます。
- KX III から更新された CIM 名は、KX III の命名規則に対応する CIM メモリ領域に保持され、この領域から取得されます。
- CIM 名が更新されても、Paragon II と KX III の間で互いに反映されることはありません。

Paragon II と KX III の間でサポートされている接続距離

KX III を Paragon II システムのフロント エンドとして使用する場合は、優れたビデオ品質が得られるようにケーブル長（距離）を制限する必要があります。

Paragon II ユーザ ステーションからターゲット サーバまでのサポートされているケーブル長は、152 m (500 フィート) です。さらに距離を延ばすと、満足できるかどうかわからないビデオ パフォーマンスになることがあります。

KX III から Paragon II ユーザ ステーションまでのサポートされているケーブル長は、最大 45 m (150 フィート) です。

KX III への Paragon II の接続

Paragon II システムを KX III に接続するには、以下の手順に従います。

1. KX III に接続する Paragon II ユーザ ステーションにバージョン 4.6 (以降) のファームウェアが実装されているかどうかを確認します。実装されていない場合は、ファームウェアをアップグレードします。

   Paragon II ユーザ ステーションは、次のいずれかです。

   - P2-UST
   - P2-EUST
   - P2-EUST/C

   アップグレード方法については、**Paragon II ヘルプ** を参照してください。
2. 互換性のある DCIM-USB を Paragon II ユーザ ステーションの USB ポートおよびビデオ ポートに接続します。

   システムが 2 層または 3 層になっている場合は、Paragon II ユーザ ステーションがベース KX III デバイス (1 層目) に接続されていることを確認します。
3. 最長 45 m (150 フィート) の Cat5 UTP ケーブルで Paragon II ユーザ ステーションを KX III に接続します。

- ケーブルの片側を DCIM の RJ-45 ポートに接続し、反対側を KX III のチャネル ポートのいずれかに接続します。

4. KX III または CC-SG で同じ Paragon II システムへのアクセス パスを増やす場合は、手順 1 〜 3 を繰り返して、さらにユーザ ステーションを KX III に接続します。

Ap C　dcTrack での KX III の管理

この章の内容

概要... 324
キャビネット内の KX III 用スペースの検索.................................... 325
dcTrack への KX III の追加 326
KX III のデータ サーキットおよび電源サーキットの作成................ 328
KX III のアイテム追加要求の送信... 329
KX III 作業工程の管理 329
キャビネット正面図およびフロア マップ図での KX III の可視化..... 329
KX III のライフサイクルの管理.. 331

概要

Raritan の dcTrack® は、設備、ネットワーク、および IT に関するリアルタイム情報を提供する、充実したデータ センタ インフラストラクチャ管理 (DCIM) ソリューションです。

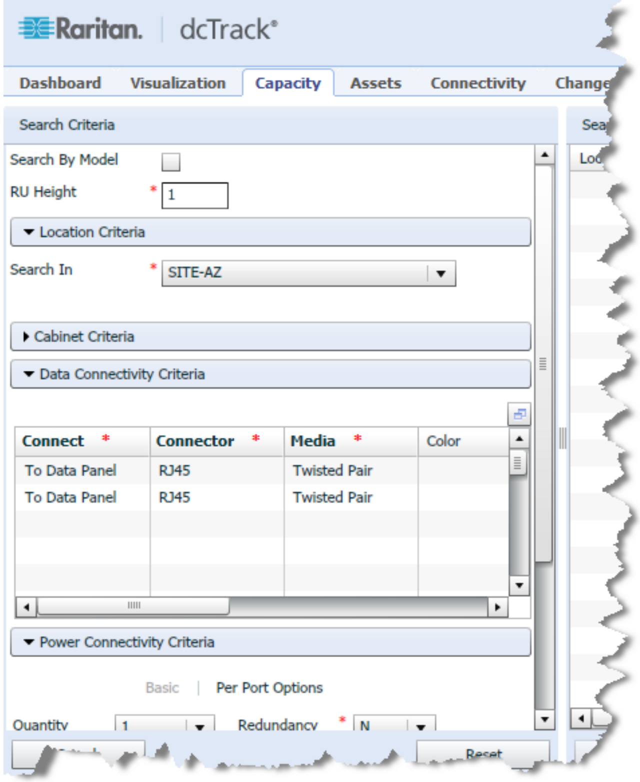
dcTrack では、データ センタや設備の管理者が IT 機器の配置の管理、情報に基くキャパシティ管理の意思決定、および KX III のようなデータ センタ資産の正確な資産管理を行いやすいように、インフラストラクチャが可視化されます。

キャビネット内の KX III 用スペースの検索

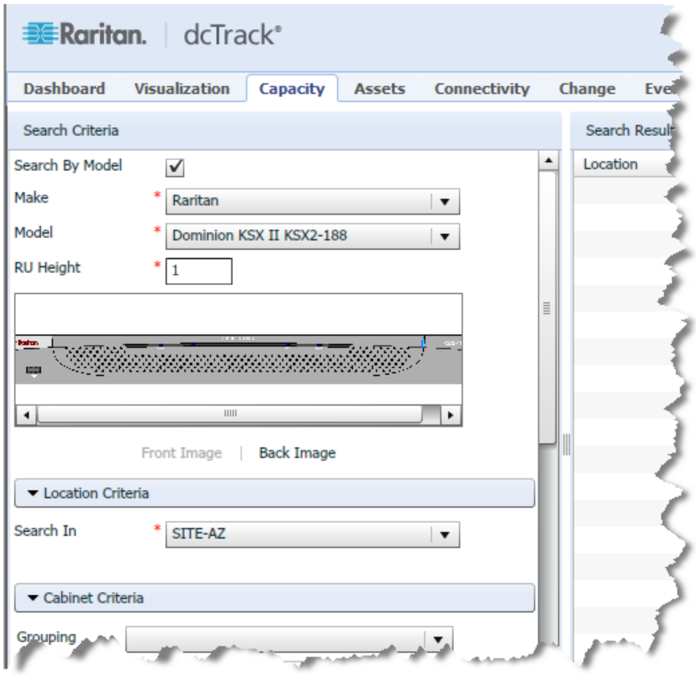
dcTrack のキャパシティ管理機能を使用して、データ センタのキャビネット内の KX III 用スペースを検索します。

検索条件:

- ラック ユニット – KX III を十分に収容可能なラック ユニットが搭載されたキャビネットを検索



- 製造元とモデル – KX III の寸法、コネクタなどに基づいて十分に収容可能なキャビネットを検索



dcTrack ヘルプの「Capacity Management – Locating and Reserving Cabinet Space for an Item (キャパシティ管理 – アイテムのキャビネット スペースの検索および確保)」を参照してください。

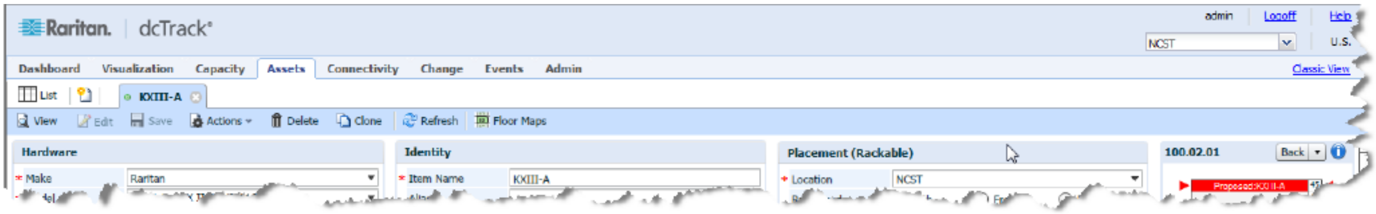
dcTrack への KX III の追加

dcTrack® で KX III を管理するには、デバイスをアプリケーションに追加します。

ニーズに基づいて dcTrack にデバイスを追加する場合は、さまざまな方法があります。

手動による dcTrack への KX III の追加

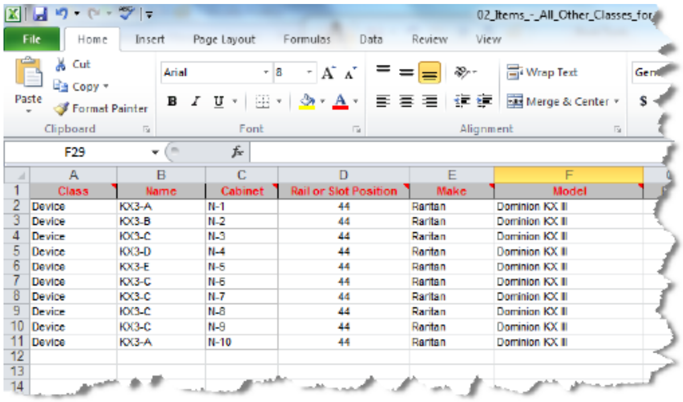
1 つまたは少数のデバイスを追加する場合は、手動で KX III を追加します。



dcTrack ヘルプの「Manually Creating New Items in dcTrack (dcTrack での手動による新規アイテムの作成)」を参照してください。

dcTrack への KX III のインポート

KX III を数多く追加する場合は、Raritan から提供されている 02_Items_-_All_Other_Classes_for_3.x.xls スプレッドシートに KX III 情報を入力し、インポート ウィザードを使用して そのスプレッドシートを dcTrack® にインポートします。

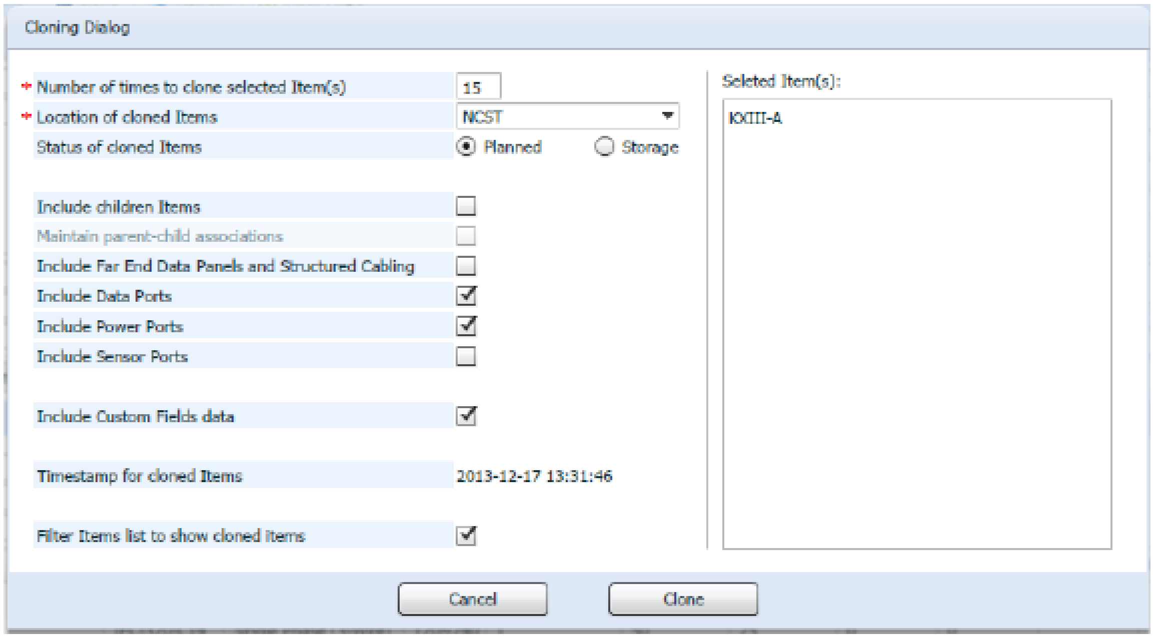


	A	B	C	D	E	F
1	Class	Name	Cabinet	Rail or Slot Position	Make	Model
2	Device	KX3-A	N-1	44	Raritan	Dominion KX III
3	Device	KX3-B	N-2	44	Raritan	Dominion KX III
4	Device	KX3-C	N-3	44	Raritan	Dominion KX III
5	Device	KX3-D	N-4	44	Raritan	Dominion KX III
6	Device	KX3-E	N-5	44	Raritan	Dominion KX III
7	Device	KX3-C	N-6	44	Raritan	Dominion KX III
8	Device	KX3-C	N-7	44	Raritan	Dominion KX III
9	Device	KX3-C	N-8	44	Raritan	Dominion KX III
10	Device	KX3-C	N-9	44	Raritan	Dominion KX III
11	Device	KX3-A	N-10	44	Raritan	Dominion KX III

dcTrack ヘルプの「Adding New Items to dcTrack Using the Import Wizard (インポート ウィザードによる dcTrack への新規アイテムの追加)」を参照してください。

既存の KX III の複製

KX III を既に追加しており、その電源サーキットやデータ サーキット (作成済みの場合)、ポート、カスタム フィールドなどに従って複製する場合は、複製機能を利用します。



キャビネット全体 (キャビネット内のアイテムを含む)、およびその接続と子デバイスも複製されます。

そのため、KX III をキャビネットに追加して、データ センタ全体で同じキャビネット構成にする場合は、キャビネットを複製できます。

dcTrack ヘルプの「Creating New Items and Cabinets Using Cloning (複製によるアイテムおよびキャビネットの新規作成)」を参照してください。

KX III のデータ サーキットおよび電源サーキットの作成

KX III が dcTrack® に存在する場合は、そのデータ サーキットおよび電源サーキットを作成します。

サーキットは、KX III を追加するとき、または後から作成できます。

サーキットが作成されたら、データ センタでサーキットを作成する要求を発行します。

dcTrack ヘルプの「Building New Circuits for Items (アイテムのサーキットの新規作成)」を参照してください。

KX III のアイテム追加要求の送信

dcTrack® に KX III を追加したら、アイテムの設置要求を送信します。

この要求により、データ センタに KX III を物理的に設置する作業工程から始まる変更管理プロセスが開始されます。

dcTrack ヘルプの「Submit an Install Item Request from the Action Menu ([Action] (アクション) メニューからアイテムの設置要求の送信)」を参照してください。

KX III 作業工程の管理

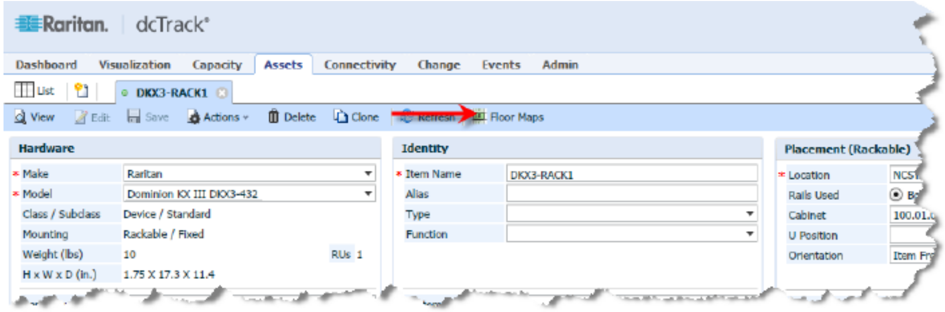
要求回避モードが有効になっておらず、アイテム要求の移動が生じる変更管理プロセスが dcTrack® で管理されていない場合、KX III の設置の作業工程は、dcTrack Gatekeeper で管理されます。

dcTrack ヘルプの「Managing Work Orders (作業工程の管理)」または「Request Bypass (要求回避)」を参照してください。

キャビネット正面図およびフロア マップ図での KX III の可視化

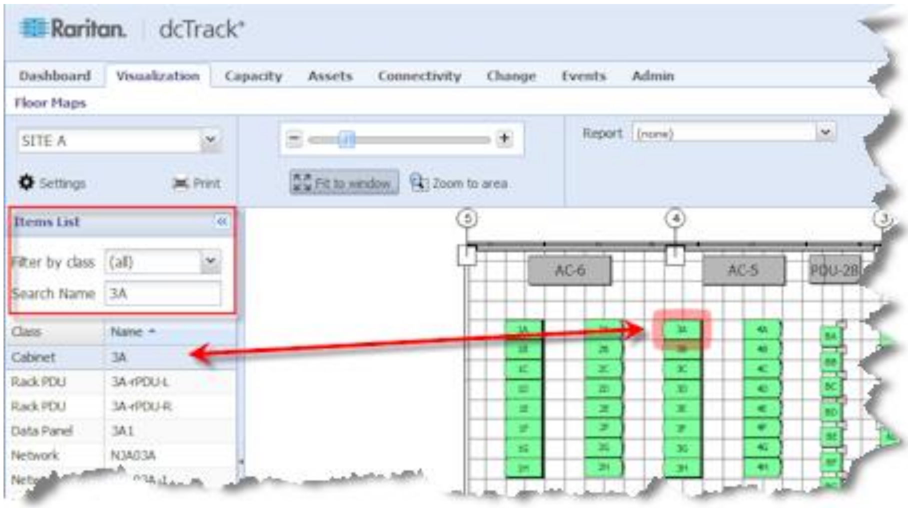
dcTrack® に KX III を追加する場合は、KX III をキャビネット内に配置します。

データ センタのキャビネットの場所にフロア マップが関連付けられており、KX III を収容するキャビネットがフロア マップ上のキャビネット オブジェクトにリンクされている場合は、dcTrack で KX III のページからフロア マップにアクセスできます。



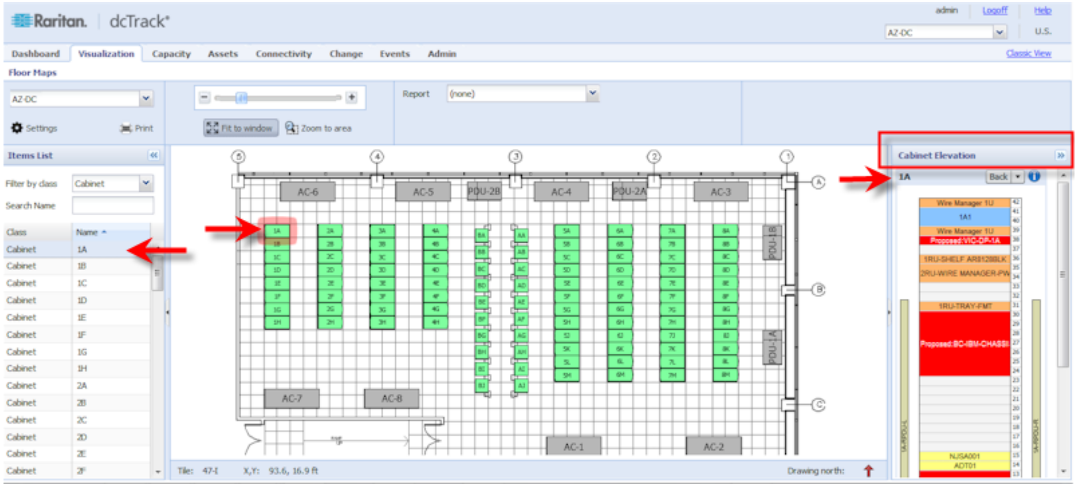
dcTrack ヘルプの「Open a Floor Map from an Item's Page (アイテムのページからフロア マップを開く)」を参照してください。

フロア マップ ページでは、フロア マップ上および [Items List] (アイテム リスト) に、KX III が収容されるキャビネットの場所が表示されます。



dcTrack ヘルプの「Locate an Item on the Floor Map and Items List (Web Client) (フロア マップおよびアイテム リストでのアイテムの表示 (Web クライアント))」を参照してください。

また、フロア マップから KX III をキャビネット正面図で表示することもできます。



dcTrack ヘルプの「Cabinet Elevations - Floor Map (Web Client) (キャビネット正面図 - フロア マップ (Web クライアント))」を参照してください。

KX III のライフサイクルの管理

KX III を設置した後、データ センタでの KX III のライフサイクルを管理します。

KX III の移動

KX III の以下の移動要求を送信します。

- あるキャビネットから別のキャビネットへの移動
- ある場所から別の場所への移動
- あるレール位置から別のレール位置への移動

dcTrack ヘルプの「**Move Item Requests (アイテムの移動要求)**」を参照してください。

KX III の電源オン/オフ

必要に応じて、KX III の電源オン/オフの要求を送信します。

dcTrack ヘルプの「**Submitting Requests to Power On or Off Devices (デバイスの電源オン/オフの要求の送信)**」を参照してください。

KX III の有効化/有効化

KX III の有効化/有効化の要求を送信します。たとえば、保守上の理由から、一時的に取り外す場合に送信します。

dcTrack ヘルプの「**Submitting Requests to Take Items On and Off Site (アイテムの有効化/有効化の要求の送信)**」を参照してください。

KX III の使用停止と保管

KX III をオフサイトの場所に一時的に移動する場合は、KX III の使用停止と保管の要求を送信します。

dcTrack ヘルプの「**Submit a Request to Decommission an Item to Storage (アイテムの使用停止と保管の要求の送信)**」を参照してください。

KX III の使用停止とアーカイブ

処分目的で在庫から KX III を削除するには、KX III の使用停止とアーカイブの要求を送信します。

dcTrack ヘルプの「**Decommissioning an Installed Item to Archive (設置されたアイテムの使用停止とアーカイブ)**」を参照してください。

Ap D　仕様

この章の内容

ハードウェア 332
ソフトウェア 355

ハードウェア

KX III の寸法および物理的仕様

Dominion KX III モデル	説明	電源と発熱量	寸法 (W x D x H)	重量	動作温度	湿度
DKX3-108	▪ 8 サーバ ポート ▪ 1 リモート ユーザ ▪ 1 ローカル ポート (ラックで使用)	二重化電源 110 V/240 V、50 ～ 60 Hz 1.8 A、60 W、52 KCAL	17.3 x 13.15 x 1.73 インチ	8.60 lbs	0º ～ 45º C	0 ～ 85 % RH
			439 x 334 x 44 mm	3.9kg	32º ～ 113º F	
DKX3-116	▪ 16 サーバ ポート ▪ 1 リモート ユーザ ▪ 1 ローカル ポート (ラックで使用)	二重化電源 110 V/240 V、50 ～ 60 Hz 1.8 A、60 W、52 KCAL	17.3 x 13.15 x 1.73 インチ	8.60 lbs	0º ～ 45º C	0 ～ 85 % RH
			439 x 334 x 44 mm	3.9kg	32º ～ 113º F	
DKX3-132	▪ 32 サーバ ポート ▪ 1 リモート ユーザ ▪ 1 ローカ	二重化電源 110 V/240 V、50 ～ 60 Hz 1.8 A、60 W、52 KCAL	17.3 x 13.15 x 1.73 インチ	8.60 lbs	0º ～ 45º C	0 ～ 85 % RH
			439 x 334 x 44 mm	3.9kg	32º ～ 113º F	

Dominion KX III モデル	説明	電源と発熱量	寸法 (W x D x H)	重量	動作温度	湿度
	ル ポート（ラックで使用）					
DKX3-216	▪ 16 サーバ ポート ▪ 2 リモート ユーザ ▪ 1 ローカル ポート（ラックで使用）	二重化電源 110 V/240 V、50 ～ 60 Hz 1.8 A、60 W、52 KCAL	17.3 x 13.15 x 1.73 インチ 439 x 334 x 44 mm	9.08 lbs 4.12kg	0º ～ 45º C 32º ～ 113º F	0 ～ 85 % RH
DKX3-232	▪ 32 サーバ ポート ▪ 2 リモート ユーザ ▪ 1 ローカル ポート（ラックで使用）	二重化電源 110 V/240 V、50 ～ 60 Hz 1.8 A、60 W、52 KCAL	17.3 x 13.15 x 1.73 インチ 439 x 334 x 44 mm	9.08 lbs 4.12kg	0º ～ 45º C 32º ～ 113º F	0 ～ 85 % RH
DKX3-416	▪ 16 サーバ ポート ▪ 4 リモート ユーザ ▪ 1 ローカル ポート（ラックで使用）	二重化電源 110 V/240 V、50 ～ 60 Hz 1.8 A、60 W、52 KCAL	17.3 x 13.15 x 1.73 インチ 439 x 334 x 44 mm	9.08 lbs 4.12kg	0º ～ 45º C 32º ～ 113º F	0 ～ 85 % RH
DKX3-432	▪ 32 サーバ ポート	二重化電源 110 V/240 V、50 ～ 60	17.3 x 13.15 x 1.73 インチ	9.08 lbs	0º ～ 45º C	0 ～ 85 % RH

Dominion KX III モデル	説明	電源と発熱量	寸法 (W x D x H)	重量	動作温度	湿度
	▪ 4 リモート ユーザ ▪ 1 ローカル ポート（ラックで使用）	Hz 1.8 A、60 W、52 KCAL	439 x 334 x 44 mm	4.12kg	32º ～ 113º F	
DKX3-464	▪ 64 サーバ ポート ▪ 4 リモート ユーザ ▪ 1 ローカル ポート（ラックで使用）	二重化電源 110 V/240 V、50 ～ 60 Hz 1.8 A、60 W、52 KCAL	17.3 x 13.3 x 3.5 インチ	12.39 lbs	0º ～ 45º C	0 ～ 85 % RH
			439 x 338 x 89 mm	5.62kg	32º ～ 113º F	
DKX3-808	▪ 8 サーバ ポート ▪ 8 リモート ユーザ ▪ 1 ローカル ポート（ラックで使用）	二重化電源 110 V/240 V、50 ～ 60 Hz 1.8 A、60 W、52 KCAL	17.3 x 13.15 x 1.73 インチ	9.96 lbs	0º ～ 45º C	0 ～ 85 % RH
			439 x 334 x 44 mm	4.52kg	32º ～ 113º F	
DKX3-832	▪ 32 サーバ ポート ▪ 8 リモート ユーザ ▪ 1 ローカル ポート（ラックで使用）	二重化電源 110 V/240 V、50 ～ 60 Hz 1.8 A、60 W、52 KCAL	17.3 x 13.15 x 1.73 インチ	9.96 lbs	0º ～ 45º C	0 ～ 85 % RH
			439 x 334 x 44 mm	4.52kg	32º ～ 113º F	

Dominion KX III モデル	説明	電源と発熱量	寸法 (W x D x H)	重量	動作温度	湿度
DKX3-864	▪ 64 サーバ ポート ▪ 8 リモート ユーザ ▪ 1 ローカル ポート（ラックで使用）	二重化電源 110 V/240 V、50 ～ 60 Hz 1.8 A、60 W、52 KCAL	17.3 x 13.3 x 3.5 インチ	12.39 lbs	0º ～ 45º C	0 ～ 85 % RH
			439 x 338 x 89 mm	5.62kg	32º ～ 113º F	

KX III でサポートされているターゲット サーバ画面解像度

- 640x350、70Hz
- 640x350、85Hz
- 640x400、56Hz
- 640x400、84Hz
- 640x400、85Hz
- 640x480、60Hz
- 640x480、66.6Hz
- 640x480、72Hz
- 640x480、75Hz
- 640x480、85Hz
- 720x400、70Hz
- 720x400、84Hz
- 720x400、85Hz
- 800x600、56Hz
- 800x600、60Hz
- 800x600、70Hz
- 800x600、72Hz
- 800x600、75Hz
- 800x600、85Hz
- 800x600、90Hz
- 800x600、100Hz
- 832x624、75.1Hz
- 1024x768@60Hz
- 1024x768@70Hz
- 1024x768、72Hz
- 1024x768@85Hz
- 1024x768@75Hz
- 1024x768、90Hz
- 1024x768、100Hz
- 1152x864、60Hz
- 1152x864、70Hz
- 1152x864、75Hz
- 1152x864、85Hz
- 1152x870、75.1Hz
- 1280x720、60Hz
- 1280x960、60Hz
- 1280x960、85Hz

- 1280x1024@60Hz
- 1280x1024、75Hz
- 1280x1024、85Hz
- 1360x768、60Hz
- 1366x768、60Hz
- 1368x768、60Hz
- 1400x1050、60Hz
- 1440x900、60Hz
- 1600x1200、60Hz
- 1680x1050、60Hz
- 1920x1080、60Hz

ターゲット サーバのサポートされている画面解像度、接続距離、およびリフレッシュ レート

サポートされる最大接続距離は、さまざまな要素によって決まります。たとえば、Cat5 ケーブルのタイプと品質、サーバのタイプと製造元、ビデオ ドライバとモニタ、環境条件、ユーザの要求レベルなどに左右されます。

次の表に、各種の画面解像度とリフレッシュ レートにおける最大接続距離を示します。

ターゲット サーバ画面解像度	最大接続距離
1024x768、60Hz (以下)	45 m (150 フィート)
1280x1024@60Hz	30 m (100 フィート)
1280x720、60Hz	22 m (75 フィート)
1600x1200、60Hz	15 m (50 フィート)
1920x1080、60Hz	15 m (50 フィート)

KX III でサポートされている画面解像度については、「*KX III でサポートされているターゲット サーバ画面解像度* 『*336*p. 』」を参照してください。

注:サーバの製造メーカーやタイプ、OS のバージョン、ビデオ ドライバなどは多種多様であるうえ、ビデオ品質にはユーザの主観が反映されるため、Raritan ではあらゆる環境でのすべての距離におけるパフォーマンスを保証することはできません。

KX III ローカル ポートのサポートされている DVI 解像度

- 1920x1080、60Hz
- 1280x720、60Hz
- 1024x768、60Hz (デフォルト)
- 1024x768、75Hz
- 1280x1024、60Hz
- 1280x1024、75Hz
- 1600x1200、60Hz
- 800x480、60Hz
- 1280x768、60Hz
- 1366x768、60Hz
- 1360x768、60Hz
- 1680x1050、60Hz
- 1440x900、60Hz

サポートされているコンピュータ インタフェース モジュール (CIM) の仕様

デジタル CIM は、Display Data Channels (DDC) および Enhanced Extended Display Identification Data (E-EDID) に対応しています。

CIM モデル	説明	寸法 (W x D x H)	重量
D2CIM-DVUSB	デュアル USB CIM (BIOS 仮想メディア、スマートカード/CAC、音声、およびずれないマウス用)	43 x 90 x 19 mm (1.7 x 3.5 x 0.8 インチ)	0.11 kg (0.25 lb)
D2CIM-VUSB	USB CIM (仮想メディアおよびずれないマウス用)	33 x 76 x 15mm (1.3 x 3.0 x 0.6 インチ)	0.09kg (0.09kg)

CIM モデル	説明	寸法 (W x D x H)	重量
D2CIM-DVUSB-DVI	デジタルとアナログの変換を行い、仮想メディア、スマートカード/CAC、音声、絶対および相対マウス同期をサポートするデジタル CIM	43 x 90 x 19 mm (1.7 x 3.5 x 0.8 インチ)	0.11 kg (0.25 lb)
D2CIM-DVUSB-DP	デジタルとアナログの変換を行い、仮想メディア、スマートカード/CAC、音声、絶対および相対マウス同期をサポートするデジタル CIM	43 x 90 x 19 mm (1.7 x 3.5 x 0.8 インチ)	0.11 kg (0.25 lb)
D2CIM-DVUSB-HDMI	デジタルとアナログの変換を行い、仮想メディア、スマートカード/CAC、音声、絶対および相対マウス同期をサポートするデジタル CIM	43 x 90 x 19 mm (1.7 x 3.5 x 0.8 インチ)	0.11 kg (0.25 lb)
DCIM-PS2	CIM (PS2 用)	33 x 76 x 15mm (1.3 x 3.0 x 0.6 インチ)	0.09kg (0.09kg)
DCIM-USBG2	CIM (USB および Sun USB 用)	33 x 76 x 15mm (1.3 x 3.0 x 0.6 インチ)	0.09kg (0.09kg)

CIM モデル	説明	寸法 (W x D x H)	重量

キーボードおよびマウスには、DVUSB CIM の黒のコネクタが使用されています。グレーのコネクタは、仮想メディアに使用します。

CIM の両方のプラグをデバイスに接続したままにします。両方のプラグがターゲット サーバに接続されていない場合は、デバイスが正しく動作しないことがあります。

サポートされているデジタル ビデオ CIM (Mac 用)

デジタル ビデオ CIM を使用して、次の Mac® ポートに接続します。

Mac ポート	CIM
DVI	D2CIM-DVUSB-DVI
HDMI	D2CIM-DVUSB-HDMI
DisplayPort または Thunderbolt	D2CIM-DVUSB-DP

Mac の HDMI または DisplayPort ビデオがミニ コネクタになっている場合は、デジタル CIM のフル サイズの HDMI および DisplayPort プラグに接続するために、パッシブ アダプタ ケーブルが必要になることがあります。

あるいは、Mac VGA アダプタを D2CIM-VUSB または D2CIM-DVUSB と併用します。これは信頼性が低く、ビデオ品質が劣化するおそれがあることに注意してください。

Mac 対応の KX III 2.5.0 (以降) でサポートされている既定モードについては、「*デジタル CIM の既定モードおよび標準モード* 『*341*p. 』」を参照してください。

デジタル CIM タイミング モード

以下は、KX III がデジタル CIM を介してビデオ ソースとやり取りするときに使用されるデフォルトのタイミング モードです。

使用されるタイミング モードは、ビデオ ソースの本来の解像度によって異なります。

- 1920x1080、60Hz
- 1600x1200、60Hz
- 1280x1024、60Hz (デジタル CIM に適用されるデフォルトの解像度)
- 1440x900、60Hz
- 1024x768@60Hz

詳細については、オンライン ヘルプの「*CIM ポートの設定* 『*94*p. 』」を参照してください。

デジタル CIM の既定モードおよび標準モード

以下の既定の解像度とタイミング モード、および標準の解像度とタイミング モードは、KX III 3.0.0 (以降) でサポートされています。

デジタル CIM 既定モード

- 720 x 400、70Hz (IBM、VGA)
- 640 x 480、60Hz (IBM、VGA)
- 640 x 480、67Hz (Apple Mac® II)
- 640 x 480、72Hz (VESA)
- 640 x 480、75Hz (VESA)
- 800 x 600、56Hz (VESA)
- 800 x 600、60Hz (VESA)
- 800 x 600、72Hz (VESA)
- 800 x 600、75Hz (VESA)
- 832 x 624、75Hz (Apple Mac II)
- 1024 x 768、60Hz (VESA)
- 1024 x 768、70Hz (VESA)
- 1024 x 768、75Hz (VESA)
- 1280 x 1024、75Hz (VESA)
- 1152 x 870、75Hz (Apple Mac II)

デジタル CIM 標準モード

- 1152 x 864、75Hz (VESA)
- 1280 x 960、60Hz (VESA)
- 1280 x 1024、60Hz (VESA)
- 1360 x 768、60Hz (VESA)
- 1400 x 1050、60Hz (VESA)
- 1440 x 900、60Hz (VESA)
- 1600 x 1200、60Hz (VESA)
- 1680 x 1050、60Hz (VESA)
- 1920 x 1080、60Hz (VESA)

DVI 互換モード

DVI 互換モードは、Intel のビデオ カードを搭載した Dell Optiplex ターゲットまたは HDMI ビデオ ポートを搭載した Mac® Mini に HDMI CIM を使用して接続する場合に必要になる可能性があります。

このモードを選択すると、ターゲットからの優れた画質が保証されます。

オンライン ヘルプの「*CIM ポートの設定* 『*94*p. 』」を参照してください。

サポートされているリモート接続

リモート接続	詳細情報
ネットワーク	10BASE-T、100BASE-T、および 1000BASE-T (Gigabit) Ethernet
プロトコル	TCP/IP、UDP、SNTP、HTTP、HTTPS、RADIUS、LDAP/LDAPS

ネットワーク速度の設定

KX III におけるネットワーク速度の設定

		自動	1000/全二重	100/全二重	100/半二重	10/全二重	10/半二重
ネットワーク スイッチにおけるポートの設定	自動	使用可能な最高速度	1000/全二重	KX III: 100/全二重 スイッチ: 100/半二重	100/半二重	KX III: 10/全二重 スイッチ: 10/半二重	10/半二重

KX III におけるネットワーク速度の設定

1000/全二重	1000/全二重	1000/全二重	通信不可	通信不可	通信不可	通信不可
100/全二重	KX III: 100/半二重 スイッチ: 100/全二重	KX III: 100/半二重 スイッチ: 100/全二重	100/全二重	KX III: 100/半二重 スイッチ: 100/全二重	通信不可	通信不可
100/半二重	100/半二重	100/半二重	KX III: 100/全二重 スイッチ: 100/半二重	100/半二重	通信不可	通信不可
10/全二重	KX III: 10/半二重 スイッチ: 10/全二重	通信不可	通信不可	通信不可	10/全二重	KX III: 10/半二重 スイッチ: 10/全二重
10/半二重	10/半二重	通信不可	通信不可	通信不可	KX III: 10/全二重 スイッチ: 10/半二重	10/半二重

凡例:

- (白) 通信できません。
- (緑) サポート
- (水色) 通信は行えますが、推奨できません。
- (赤) Ethernet 仕様でサポートされていません。通信は行えますが、衝突が発生します。
- (太枠) Ethernet 仕様では通信できないことになっています。KX III は期待どおりに動作しません。

注:ネットワーク通信の信頼性を高めるため、KX III とネットワーク スイッチの双方で、通信速度と通信方式を同じ設定にしてください。たとえば、KX III とネットワーク スイッチで "自動検出" に設定するか (推奨)、または、双方の通信速度と通信方式を同じ設定にします (例: 100 Mbps/全二重)。

Dell 筐体を接続する場合のケーブル長と画面解像度

KX III に Dell® 製ブレード筐体を接続する場合、画質を維持するために次のケーブル長と画面解像度を使用することを推奨します。

画面解像度	ケーブル長
1024x768@60Hz	15.24 m (50 フィート)
1280x1024@60Hz	15.24 m (50 フィート)
1600x1200、60Hz	9.14 m (30 フィート)

スマート カードの最小システム要件

ローカル ポートの要件

KX III へのローカル ポート接続の相互運用性の基本要件は、以下のとおりです。

- ローカルに接続されたすべてのデバイス(スマート カード リーダーまたはトークン)は、USB CCID に準拠している必要があります。

ターゲット サーバの要件

スマート カード リーダーを使用する場合、ターゲット サーバにおける相互運用性の基本要件は以下のとおりです。

- IFD (スマート カード リーダー) Handler は、標準の USB CCID デバイス ドライバ (汎用の Microsoft® USG CCID ドライバに相当) である必要があります。
- デジタル CIM または D2CIM-DVUSB (デュアル VM CIM) が必要であり、そのファームウェア バージョンは 3A6E 以降である必要があります。
- ブレード シャーシのサーバ接続 (ブレードごとに CIM を使用) がサポートされます。
- ブレード シャーシのサーバ接続 (シャーシごとに CIM を使用) は、自動検出が有効になっている IBM® BladeCenter® モデル H および F でのみサポートされます。

Windows XP ターゲット

Windows XP® ターゲットでは、KX III でスマート カードを使用するために Windows XP SP3 が実行されている必要があります。ターゲット サーバ上の Windows XP 共有で .NET 3.5 を実行している場合、SP1 を適用する必要があります。

Linux ターゲット

Linux® ターゲットを使用している場合、Raritan デバイスでスマート カード リーダーを使用するには、以下の要件を満たす必要があります。

- CCID の要件

  Linux ターゲットで Raritan D2CIM-DVUSB VM/CCID がスマート カード リーダーとして認識されない場合は、CCID ドライバのバージョンを 1.3.8 以上に更新し、ドライバ設定ファイル (Info.plist) を更新する必要があります。

オペレーティング システム	CCID の要件
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12
Fedora® Core 10	ccid-1.3.8-1.fc10.i386

リモート クライアントの要件

リモート クライアントにおける相互運用性の基本要件は、以下のとおりです。

- IFD (スマート カード リーダー) Handler は、PC/SC 準拠のデバイス ドライバである必要があります。
- ICC (スマート カード) Resource Manager が使用可能で、PC/SC 準拠である必要があります。
- スマート カード API を含む JRE® が Raritan クライアント アプリケーションで使用可能である必要があります。

Linux リモート クライアントの要件

Linux® クライアントを使用している場合、Raritan デバイスでスマート カード リーダーを使用するには、以下の要件を満たす必要があります。

注:ターゲットへの 1 つ以上の KVM セッションがアクティブになっている場合、スマート カードを挿入すると、クライアントへのユーザ ログインに時間がかかることがあります。これらのターゲットへのログイン プロセスも進行中です。

- PC/SC の要件

オペレーティング システム	必要な PC/SC
RHEL 5	pcsc-lite-1.4.4-0.1.el5
SuSE 11	pcsc-lite-1.4.102-1.24
Fedora® Core 10	pcsc-lite-1.4.102.3.fc10.i386

- Java® ライブラリ リンクの作成

  RHEL 4、RHEL 5、および FC 10 のアップグレード後、libpcsclite.so へのソフト リンクを作成する必要があります。たとえば、パッケージのインストールによってライブラリが /usr/lib または /user/local/lib に配置される場合、「ln -s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so」と入力します。

- PC/SC デーモン

  pcsc デーモン (フレームワークのリソース マネージャ) を再起動すると、ブラウザが再起動します。

サポートされているスマート カード リーダー

タイプ	ベンダ	[Model] (モデル)	検証
USB	SCM Microsystems	SCR331	ローカルおよびリモートで検証済み
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	ローカルおよびリモートで検証済み
USB	ActivIdentity	ActivIdentity USB Reader v3.0	ローカルおよびリモートで検証済み
USB	Gemalto®	GemPC USB-SW	ローカルおよびリモートで検証済み
USB キーボード/カード リーダーの組み合わせ	Dell®	USB Smart Card Reader Keyboard	ローカルおよびリモートで検証済み
USB キーボード/カード リーダーの組み合わせ	Cherry GmbH	G83-6744 SmartBoard	ローカルおよびリモートで検証済み
SIM サイズのカードに対応した USB リーダー	Omnikey	6121	ローカルおよびリモートで検証済み
統合型 (Dell Latitude D620)	O2Micro	OZ776	リモートのみ
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	リモートのみ
PCMCIA	SCM Microsystems	SCR243	リモートのみ

注:SCM Microsystems の SCR331 スマート カード リーダーでは、SCM Microsystems のファームウェア v5.25 を使用する必要があります。

サポートされていないスマート カード リーダー

この表は、Raritan がテストし、Raritan デバイスでは動作しないことが判明しているリーダーの一覧です。したがって、これらのリーダーはサポートされていません。

サポートされているスマート カード リーダーの表にもサポートされていないスマート カード リーダーの表にもないスマート カード リーダーについては、デバイスでの動作を保証できません。

タイプ	ベンダ	[Model] (モデル)	注意
USB キーボード/カード リーダーの組み合	HP®	ED707A	インタラプト エンドポイントなし =>

タイプ	ベンダ	[Model] (モデル)	注意
わせ			Microsoft® ドライバとの互換性なし
USB キーボード/カード リーダーの組み合わせ	SCM Microsystems	SCR338	独自のカード リーダー実装（CCID 非準拠）
USB トークン	Aladdin®	eToken PRO™	独自の実装

音声の再生とキャプチャに関する推奨事項と要件

音声レベル

- ターゲットの音声レベルを中域に設定します。

  たとえば、Windows® クライアントでは、音声を 50 以下に設定します。

この設定は、クライアントの音声デバイス コントロールではなく、再生またはキャプチャ用の音声デバイスで行う必要があります。

PC 共有モードが有効になっている場合の音声接続に関する推奨事項

PC 共有モードでの動作中に音声機能を使用している場合は、さらに音声デバイスがターゲットに接続されると、音声の再生やキャプチャが中断されます。

たとえば、ユーザ A がターゲット 1 に再生デバイスを接続して音声再生アプリケーションを実行し、ユーザ B が同じターゲットにキャプチャデ バイスを接続するとします。この場合、ユーザ A の再生セッションは中断されるので、音声アプリケーションを再起動する必要があります。

この中断が発生する理由は、新しいデバイス設定で USB デバイスを再列挙する必要があるためです。

ターゲットで新しいデバイスのドライバをインストールする場合は、少し時間がかかることがあります。

音声アプリケーションは、再生の完全な停止、次のトラックへの移動、または再生の続行となる可能性があります。

正確な動作は、音声アプリケーションで切断/再接続イベントがどのように処理されるかによって異なります。

帯域幅要件

次の表は、選択した各形式で音声を転送する場合の音声再生およびキャプチャの帯域幅要件の詳細です。

音声形式	ネットワーク帯域幅要件
44.1 KHz、16 ビット ステレオ	176 kbps
44.1 KHz、16 ビット モノラル	88.2 kbps
2.05 KHz、16 ビット ステレオ	88.2 kbps
22.05 KHz、16 ビット モノラル	44.1 kbps
11.025 KHz、16 ビット ステレオ	44.1 kbps
11.025 KHz、16 ビット モノラル	音声 22.05 kbps

実際に、音声デバイスをターゲットに接続するときに使用される帯域幅は、ターゲットで音声アプリケーションを開いたり使用したりする際に消費されるキーボード データやビデオ データがあるため、広くなっています。

一般的には、再生およびキャプチャを実行する前に、1.5 MB 以上の接続を維持していることを推奨します。

ただし、ターゲット画面の解像度を高くして高品質なビデオ コンテンツをフル カラー接続すると、さらに多くの帯域幅を消費するため、音声の品質が大幅に劣化します。

品質の低下を軽減できるように、帯域幅が狭い場合にビデオが音声品質に与える影響を軽減するための推奨のクライアント設定は数多くあります。

- 音声の再生を低品質の形式で接続します。帯域幅を消費するビデオによる影響は、44k よりも 11k で接続した方が大幅に減少します。
- [Connection Properties] (接続プロパティ) で、接続速度を、クライアントからサーバへの接続に最適な値に設定します。
- [Connection Properties] (接続プロパティ) で、色深度をできる限り低い値に設定します。色深度を 8 ビット カラーにすると、消費される帯域幅が大幅に減少します。
- [Smoothing] (スムージング) を [High] (高) に設定します。これにより、表示されるビデオ ノイズが減少し、ターゲット ビデオの画質が向上します。
- [Video] (ビデオ) 設定で、[Noise Filter] (ノイズ フィルタ) を最も高い設定 7 (最高値) にすると、ターゲットの画面変更に使用される帯域幅が小さくなります。

Mac 環境での音声

以下は、Mac® 環境での既知の問題です。

- Mac クライアントで、Virtual KVM Client (VKC) からデバイスにアクセスすると、[Connect Audio] (音声に接続) パネルに再生デバイスが 1 つだけリストされます。リストされたデバイスはデフォルトであり、[Connect Audio] (音声に接続) パネルに「Java Sound Audio Engine」として表示されます。
- Mac ターゲットで Skype® を介して音声を使用すると、音声が破損する可能性があります。

サポートされている音声/仮想メディアおよびスマート カード接続の数

クライアントからターゲットに確立する音声/仮想メディア、およびスマート カードの同時接続数を以下に示します。

- 1 スマート カード
- 1 仮想メディア
- 1 スマート カードおよび 1 仮想メディア
- 2 仮想メディア

各言語に対して KX III でサポートされているキーボード

次の表に、各言語に対して KX III でサポートされているキーボードを示します。

*注:中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。アメリカ英語以外のキーボードの詳細については、「***留意事項** *『359p.』」を参照してください。*

注:Linux 環境で作業する場合は、system-config-keyboard を使用して言語を変更することをお勧めします。

言語	地域	キーボード レイアウト
US 英語	米国および大半の英語圏の諸国: カナダ、オーストラリア、ニュージーランドなど	US キーボード レイアウト
US インターナショナル	米国および大半の英語圏の諸国: オランダなど	US キーボード レイアウト
UK 英語	英語 (イギリス)	UK レイアウト キーボード
繁体字中国語	香港、中国 (台湾)	繁体字中国語
簡体字中国語	中国	簡体字中国語
韓国語	韓国	Dubeolsik ハングル
日本語	日本	JIS キーボード
[French] (フランス語)	フランス	フランス語 (AZERTY) レイアウト キーボード
[German] (ドイツ語)	ドイツおよびオーストリア	ドイツ語キーボード (QWERTZ レイアウト)

言語	地域	キーボード レイアウト
[French] (フランス語)	ベルギー	ベルギー語 (ベルギー)
ノルウェー語 (ノルウェー)	ノルウェー	ノルウェー語 (ノルウェー)
デンマーク語 (デンマーク)	デンマーク	デンマーク語 (デンマーク)
スウェーデン語 (スウェーデン)	スウェーデン	スウェーデン語 (スウェーデン)
ハンガリー語	ハンガリー	ハンガリー語
スロベニア語	スロベニア	スロベニア語
イタリア語	イタリア	イタリア語
スペイン語	スペインおよび大半のスペイン語圏の諸国	スペイン語
ポルトガル語	ポルトガル	ポルトガル語

Mac Mini BIOS のキー入力コマンド

以下の BIOS コマンドは、Mac Snow Leopard® が稼動している Intel ベースの Mac® Mini ターゲット サーバおよび Mac Lion® サーバ上でテストされたものです。これらのサーバは、D2CIM-DVUSB および D2CIM-VUSB CIM で KX III に接続されました。サポートされているキーおよび留意事項については、下記を参照してください。

キー入力	説明	仮想メディア CIM	デュアル仮想メディア CIM	Mac Lion サーバ HDMI CIM
起動時に C キーを押す	起動可能な CD または DVD (Mac OS X インストール ディスクなど) から起動する	✓	✓	
起動時に D キーを押す	Apple Hardware Test (AHT) で起動します。	✓ Mac のマウス用の正常に機能する BIOS プロファイ	✓ Mac のマウス用の正常に機能する BIOS プロフ	✓ Mac のマウス用の正常に機能する BIOS プロフ

キー入力	説明	仮想メディア CIM	デュアル仮想メディア CIM	Mac Lion サーバ HDMI CIM
		ルを必要とする場合がある	ァイルを必要とする場合がある	ァイルを必要とする場合がある
2 回目の起動音が聞こえるまで Option-Command-P-R キーを押す	NVRAM をリセットします。		✓	✓
起動時に Option キーを押す	スタートアップ マネージャで起動。起動元の Mac OS X ボリュームを選択できる	✓	✓	✓
イジェクト キーまたは F12 キーを押すか、マウス ボタンを押し続ける	リムーバブル メディア (光学ディスクなど) を取り出す	✓	✓	
起動時に N キーを押す	互換性のあるネットワーク サーバから起動する (NetBoot)	✓	✓	✓
起動時に T キーを押す	ターゲット ディスク モードで起動する			✓
起動時に Shift キーを押す	セーフ モードで起動し、ログイン項目を一時的に無効にします。	✓	✓	Lion をセーフ モードで起動する際の既知の問題点。Lion では、赤字の "セーフ ブート" が表示されない
起動時に Command-V キーを押す	Verbose mode.admin で起動する	✓	✓	✓
起動時に Command-S キーを押す	シングル ユーザ モードで起動します。	✓	✓	✓
起動時に Option-N キーを押す	デフォルトのブート イメージを使用して NetBoot サーバから起動します。	✓	✓	✓

キー入力	説明	仮想メディア CIM	デュアル仮想メディア CIM	Mac Lion サーバ HDMI CIM
起動時に Command-R キーを押す	Lion Recovery から起動します。	なし	なし	✓

Windows キーボードによる Mac ターゲットへのアクセス

Windows® キーボードを使用して、KX III に接続されている Mac® にアクセスできます。Windows キーで、特殊な Mac キーをエミュレートします。これは、Windows キーボードを Mac に直接接続するのと同じことです。

使用される TCP ポートおよび UDP ポート

ポート	説明
HTTP、ポート 80	このポートは、必要に応じて設定できます。「*HTTP ポートおよび HTTPS ポートの設定* 『*134*p. 』」を参照してください。 セキュリティを確保するため、デフォルトでは、KX III によって HTTP (ポート 80) で受信された要求は、すべて HTTPS に自動変換されます。 要求はポート 80 で受け付けられるので、ユーザはブラウザのアドレス ボックスに明示的に「https://」と入力する必要はありません。また、セキュリティも確保されます。
HTTP、ポート 443	このポートは、必要に応じて設定できます。「*HTTP ポートおよび HTTPS ポートの設定* 『*134*p. 』」を参照してください。 デフォルトでは、このポートはさまざまな目的で使用されます。たとえば、クライアントから HTML で Web サーバにアクセスする場合、クライアント ソフトウェア (Virtual KVM Client (VKC)) をクライアントにダウンロードする場合、KVM データと仮想メディア データをクライアントに転送する場合などです。
KX III (Raritan KVM-over-IP) プロトコル、ポート 5000 (変更可)	このポートは、他の Dominion デバイスの検出、および Raritan デバイスと各種システム (CC-SG 管理で利用可能なデバイス向けの CC-SG など) との間の通信に使用されます。 このポートはデフォルトで 5000 に設定されていますが、別の TCP ポートに変更することもできます。この設定を変更する手順については、「*ネットワーク設定* 『*84*p. 』」を参照してください。
SNTP (時刻サーバ)、UDP ポート 123 (変更可)	KX III の内部クロックを中央の時刻サーバと同期させることができます。 この機能を利用するには UDP ポート 123 (SNTP 用の標準ポート) を

ポート	説明
	使用する必要がありますが、別のポートに変更することもできます。**(オプション)**
LDAP/LDAPS、ポート 389 または 636 (変更可)	LDAP/LDAPS プロトコルを使用してユーザをリモート認証するように KX III LDAP/LDAPS プロトコルを使用してユーザをリモート認証するように KX III が設定されている場合、デフォルトでポート 389 または 636 が使用されます。ただし、別のポートに変更することもできます。**(オプション)**
RADIUS、ポート 1812 (変更可)	RADIUS プロトコルを使用してユーザをリモート認証するように KX III が設定されている場合、デフォルトでポート 1812 が使用されます。ただし、別のポートに変更することもできます。**(オプション)**
設定可能なポート 1813 を使用する RADIUS アカウンティング	RADIUS プロトコルを使用してユーザをリモート認証するように KX III が設定されており、かつ、イベントのログ記録に RADIUS アカウンティングが使用されている場合、ログ通知の転送にデフォルトでポート 1813 が使用されます。ただし、別のポートに変更することもできます。
SYSLOG、UDP ポート 514 (変更可)	メッセージを Syslog サーバに送信するように KX III が設定されている場合、通信にデフォルトでこのポートが使用されます。ただし、別のポートに変更することもできます。
SNMP、デフォルトの UDP ポート	送受信の読み取り/書き込み SNMP アクセスにはポート 161 が使用されます。SNMP トラップの送信トラフィックにはポート 162 が使用されます。**(オプション)**
TCP ポート 22	ポート 22 は、KX III のコマンド ライン インタフェース (CLI) を利用する際に使用されます (お客様が Raritan のテクニカル サポート部門と協力して作業する場合)。
SSH	SSH (Secure Shell) ポートは設定できます。デフォルトはポート 22 です。

ソフトウェア

サポートされているオペレーティング システムとブラウザ

オペレーティング システム	ブラウザ
Windows 7® Home Premium SP1 64 ビット	▪ Internet Explorer® 10 および 11 ▪ Firefox® 25 ▪ Chrome® 31 ▪ Safari® 5.1.7

オペレーティング システム	ブラウザ
Windows 7 Ultimate SP1 64 ビット	▪ Internet Explorer 8、9、11 ▪ FireFox 25 ▪ Chrome 31
Windows 7 Ultimate 32 ビット	▪ Internet Explorer 8 ▪ FireFox 25 ▪ Chrome 31
Windows 8® 64 ビット	▪ Internet Explorer 10 ▪ FireFox 25 ▪ Chrome 31
Windows Server 2012® Standard 64 ビット	▪ Internet Explorer 10 ▪ FireFox 25 ▪ Chrome 31
Windows XP® Home Edition SP 3	▪ Internet Explorer 10 ▪ FireFox 25 ▪ Chrome 31
openSUSE® 11.4 Celadon (x86_64)	▪ Firefox 16.0.2
Fedora® 18 (Spherical Cow)	▪ FireFox 24
RHEL 6.4	▪ FireFox 21
OS X Mountain Lion® 10.8.5 *	▪ Firefox 25 (推奨) ▪ Safari 6.1
Solaris® 10 64 ビット	▪ Firefox 3.6.23
Mac® 10.7.5	▪ Safari 6.0.5 ▪ FireFox 25

**注: OS X 10.8.2 から OS X 10.8.3 にアップグレードすると、Safari® で Java™ がブロックされる場合があります。*

Mac の JRE の要件およびブラウザに関する注意事項

Mac の Java Runtime Environment の要件

Virtual KVM Client (VKC) を使用して KX III 経由でターゲット サーバにアクセスする場合は、PC および Mac® に Java Runtime Environment 7 (JRE)® をインストールします。

ターゲット サーバ/PC/Mac にリモート アクセスするときに、高パフォーマンスで KVM-over-IP ビデオ処理を行うためには、この方法が確実です。

Mac 用の JRE の最新バージョンは、Apple サポート Web サイトからダウンロードできます。

Mac のブラウザに関する注意事項

特定のブラウザでは、Java がデフォルトで無効になっている場合があります。KX III を使用するためには、Java を有効にしてすべてのセキュリティ警告を承諾します。

特定のバージョンの Safari® では、セキュリティ上の理由から Java がブロックされます。KX III を使用するには、Java が必要なので、代わりに Firefox® を使用することをお勧めします。

さらに、場合によっては、多くのメッセージを参照する必要があります。こうしたメッセージが表示される場合は、[ブロックしない] を選択します。

Java および Microsoft .NET の要件

Java® 1.7 (以降) または Microsoft .NET® 3.5 (以降) では、KX III を使用する必要があります。

KX III では、現在の Java バージョンが確認され、適合していない場合は、更新するよう求められます。

詳細については、「*Java Runtime Environment (JRE) に関する留意事項*『*359*p. 』」を参照してください。

多言語対応キーボードの JRE の要件

多言語対応のキーボードを KX III および Virtual KVM Client (VKC) で使用できるようにするには、多言語バージョンの JRE™ をインストールする必要があります。

監査ログおよび Syslog でキャプチャされるイベント

KX III の監査ログと syslog でキャプチャされるイベントの一覧と説明は以下のとおりです。

- Access Login (アクセス ログイン) – ユーザが KX III にログインしました。
- Access Logout (アクセス ログアウト) – ユーザが KX III からログアウトしました。
- Active USB Profile (アクティブ USB プロファイル) – USB プロファイルがアクティブになりました。
- CIM Connected (CIM 接続) – CIM が接続されました。
- CIM Disconnected (CIM 切断) – CIM が切断されました。
- Connection Lost (切断) – ターゲットへの接続が切断されました。
- Disconnected User (ユーザの切断) – ユーザがポートから切断されました。
- End CC Control (CC 制御終了) – CC-SG 管理対象から除外されました。
- Login Failed (ログイン失敗) – ユーザのログインが失敗しました。
- Password Changed (パスワード変更) – パスワードが変更されました。
- Port Connect (ポート接続) – ポートが接続されました。
- Port Disconnect (ポート切断) – ポートが切断されました。
- Port Status Change (ポート ステータス変更) – ポート ステータスが変更されました。
- Scan Started (スキャン開始) – ターゲットのスキャンが開始されました。
- Scan Stopped (スキャン停止) – ターゲットのスキャンが停止されました。
- Session Timeout (セッション タイムアウト) – セッション タイムアウトが発生しました。
- VM Image Connected (VM イメージ接続) – VM イメージが接続されました。
- VM Image Disconnected (VM イメージ切断) – VM イメージが切断されました。

Ap E　留意事項

この章の内容

概要 359
Java Runtime Environment (JRE) に関する留意事項 359
IPv6 のサポートに関する注意事項 361
デュアル スタック ログインのパフォーマンスに関する問題 362
CIM に関する留意事項 362
仮想メディアに関する留意事項 364
USB ポートおよびプロファイルに関する留意事項 367
ビデオ モードと解像度に関する留意事項 369
キーボードに関する留意事項 370
マウスに関する留意事項 374
音声 375
スマート カードに関する留意事項 376
CC-SG に関する留意事項 376
ブラウザに関する留意事項 376

概要

この章では、KX III の使用に関する重要事項について説明します。今後更新される情報については、弊社 Web サイトで提供されます。更新情報を表示するには、KX III リモート コンソールの [Help] (ヘルプ) リンクをクリックしてください。

注:このセクションの一部のトピックでは、記載されている情報がさまざまなデバイスに影響を与えるため、他の複数の Raritan デバイスにも言及しています。

Java Runtime Environment (JRE) に関する留意事項

Java のキャッシュ機能の無効化および Java キャッシュのクリア

Microsoft Windows® の Java のキャッシュ機能を無効にし、Java™ キャッシュをクリアすることを強くお勧めします。

▶ **Java のキャッシュ機能を無効にしてキャッシュをクリアするには、以下の手順に従います。**

1. Windows の [スタート] メニューの [コントロール パネル] をクリックします。
2. Java アイコンをダブルクリックして、起動します。[Java コントロール パネル] ダイアログ ボックスが表示されます。

3. Java キャッシングを無効にするには、以下の手順に従います。
   a. [一般] タブで [設定] ボタンをクリックします。[一時ファイルの設定] ダイアログ ボックスが表示されます。
   b. [アプレットの表示] ボタンをクリックします。Java Applet キャッシュ ビューアが開きます。
   c. [キャッシュを有効にする] チェックボックスがオンになっている場合は、オフにします。
   d. [OK] をクリックします。
4. Java キャッシュをクリアするには、以下の手順に従います。
   a. [一時ファイルの設定] ダイアログ ボックスで、[ファイルの削除] ボタンをクリックします。[一時ファイルの削除] ダイアログ ボックスが表示されます。
   b. 削除する一時ファイルを選択します。
   c. [OK] をクリックします。

Java が Mac に正しくロードされていない場合

Mac® を使用しており、KX III ポート アクセスの表のデバイスに接続するときに、次のメッセージが表示される場合は、Java™ が正しくロードされていません。

"Error while getting the list of open targets, please try again in a few seconds. (開かれているターゲットのリストの取得中にエラーが発生しました。少ししてから、もう 1 度試してください。)"

このエラーが発生する場合は、インストールされている Java を次の Web サイトから確認します。

http://www.java.com/en/download/testjava.jsp

http://www.java.com/en/download/testjava.jsp

Java アプレットが非アクティブの場合は、このページから有効にすることができます。Java が正しくインストールされていない場合は、メッセージでわかるので、Java を再インストールできます。

IPv6 のサポートに関する注意事項

オペレーティング システムの IPv6 のサポートに関する留意事項

Java

Java™ 1.7 では、次のオペレーティング システム (OS) に対して IPv6 がサポートされています。

- Solaris™ 10 (以降)
- Linux® カーネル 2.1.2 (以降)/RedHat 6.1 (以降)
- Solaris 10 (以降)
- Windows XP® SP1、Windows 2003®、Windows Vista®、および Windows 7

Java では、次の IPv6 構成は*サポートされていません*。

- Microsoft® Windows® 上の J2SE では、IPv6 はサポートされていません。

Linux

- IPv6 を使用する場合、Linux カーネル 2.4.0 以降を使用することを推奨します。
- IPv6 対応のカーネルをインストールするか、または、IPv6 関連オプションを有効にしてカーネルを再ビルドする必要があります。
- IPv6 を使用する場合、Linux 用のネットワーク ユーティリティをいくつかインストールする必要があります。詳細については、http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html を参照してください。

Windows

- Windows XP ユーザや Windows 2003 ユーザは、Microsoft の IPv6 対応サービス パックをインストールし、IPv6 を有効にする必要があります。
- Windows XP に IPv6 を搭載した AKC の場合は、ファイアウォールの例外リストに実行可能ファイル kxgui.exe を追加します。クライアントのログ ファイルを表示し、ファイル kxgui.exe の場所の完全パスを確認します。

Samba

- Samba を使用する場合、IPv6 と仮想メディアを併用することはできません。

AKC ダウンロード サーバ証明書検証の IPv6 サポートに関する留意事項

If you are connecting to a KX III standalone device and support for AKC download server certificate validation is enabled, the valid IPv6 format to generate the certificate is either:

- `CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]` when there is a leading 0

  or

- `CN =[fd07:02fa:6cff:2500:020d:5dff:0000:01c0]` when there is no zero compression

デュアル スタック ログインのパフォーマンスに関する問題

デュアル スタック構成で KX III を使用している場合は、ログイン時の遅延を回避するために、KX III でドメイン システム (DNS) を正しく設定する必要があります。

KX III での DNS の設定方法については、「*Web ブラウザ インタフェースの追加に関するヒント* 『*115*p. 』」を参照してください。

CIM に関する留意事項

Linux ターゲット サーバに対して Windows の 3 ボタン マウスを使用する場合

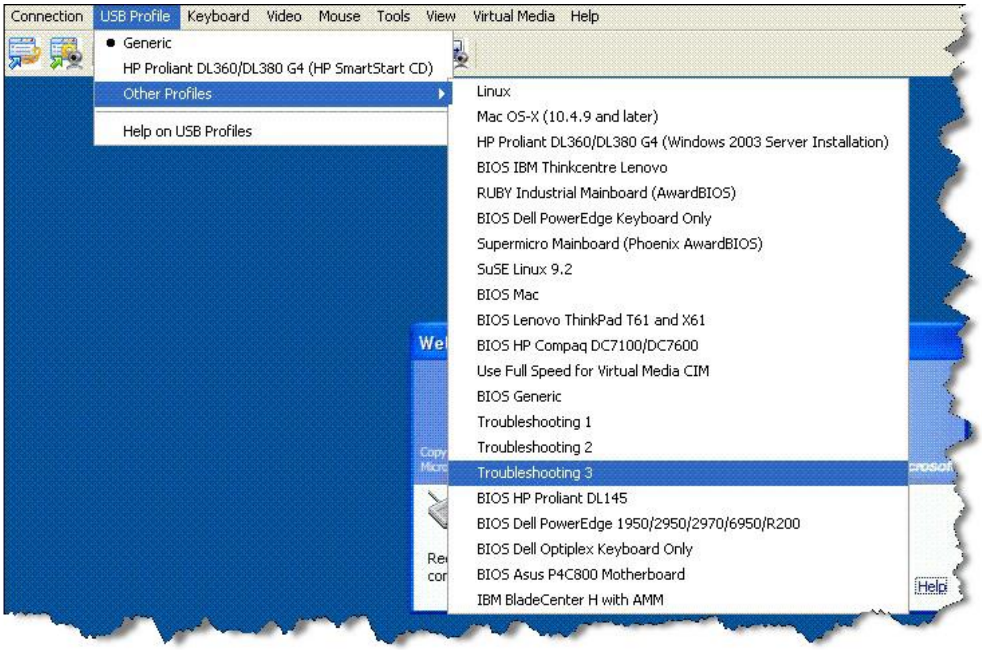
Linux® ターゲット サーバに接続している Windows® クライアントで 3 ボタン マウスを使用する場合、左マウス ボタンがその 3 ボタン マウスの中央ボタンに対応付けられることがあります。

Windows 2000 での複合 USB デバイスの動作

Windows 2000® では、Raritan の D2CIM-VUSB のような複合 USB デバイスはサポートされていないので、非複合 USB デバイスと同じように扱われます。

したがって、D2CIM-VUSB によってマッピングされているドライブに対する [Safely Remove Hardware] (ハードウェアの安全な取り外し) アイコンがシステム トレイに表示されません。また、D2CIM-VUSB を取り外す際、警告メッセージが表示されることがあります。ただし、Raritan が確認したところでは、このメッセージが表示されても何の問題も発生しません。

米国にある Raritan の設計部門は、この [Safely Remove Hardware] (ハードウェアの安全な取り外し) アイコンを表示すると共にこの警告メッセージの表示を回避するための構成を考え出しました。この構成では、D2CIM-DVUSB 仮想メディア アダプタと "Troubleshooting 3" USB プロファイルを使用する必要があります。この USB プロファイルは、D2CIM-DVUSB を、仮想メディア接続を 1 本しかサポートしない非複合 USB デバイスとして設定するものです。Raritan は、米国と日本でこの構成を十分にテストしました。



仮想メディアに関する留意事項

Linux クライアントからドライブに接続できない場合

Linux® Fedora™ 18 と Java™ 1.7.0 (update 45 以降) が稼働しているクライアントから接続するときに、ターゲット サーバの仮想メディア ドライブに接続できない場合は、クライアントで Fedora 18 の SELinux を無効にして問題を解決してください。

Mac クライアントからファイルの読み書きができない場合

Safari® 6.1 と Java™ 1.7 が稼働している Mac® 10.8.5 クライアントから KX III に接続しており、ターゲット サーバのファイルの読み書きができない場合や、仮想メディアにアクセスできない場合は、以下の手順に従って修正してください。

1. Safari で、[環境設定] を選択します。
2. [セキュリティ] タブで、[Web サイト設定を管理] を選択します。
3. "KX3 の Web サイト" をクリックします。
4. ドロップダウンから [安全でないモードで実行] を選択します。
5. Safari を再起動します。

Windows 環境での VKC および AKC を介した仮想メディア

Windows XP® の Administrator 権限および標準ユーザ権限は、Windows Vista® および Windows 7® とは異なります。

Vista または Windows 7 でユーザ アクセス制御 (UAC) を有効にすると、ユーザがアプリケーションの実行に必要とする最低レベルの権限が与えられます。たとえば、Internet Explorer® でユーザに管理者レベルのタスクの実行を明示的に許可するための [管理者として実行] オプションが用意されています。このオプションを使用しない場合、ユーザは管理者としてログインしていても管理者レベルのタスクを実行できません。

どちらの機能も、ユーザが Virtual KVM Client (VKC) および Active KVM Client (AKC) を使用してアクセスできる仮想メディアのタイプに影響します。これらの機能の詳細および使用方法については、Microsoft® のヘルプを参照してください。

ユーザが Windows 環境で VKC および AKC を使用してアクセスできる仮想メディアのタイプを以下に示します。機能をクライアント別に分類し、各 Windows ユーザ役割がアクセスできる仮想メディア機能を示します。

Windows XP

VKC および AKC を Windows XP 環境で実行している場合、CD-ROM 接続、ISO、および ISO イメージを除く仮想メディア タイプにアクセスするには、ユーザに管理者権限が必要です。

Windows Vista および Windows 7

VKC および AKC を Windows Vista または Windows 7 環境で実行し、UAC が有効になっている場合は、ユーザの Windows 役割に応じて以下の仮想メディア タイプにアクセスできます。

クライアント	管理者	標準ユーザ
AKC および VKC	アクセス先: • 固定ドライブと固定ドライブ パーティション • リムーバブル ドライブ • CD/DVD ドライブ • ISO イメージ • リモート ISO イメージ	アクセス先: • リムーバブル ドライブ • CD/DVD ドライブ • ISO イメージ • リモート ISO イメージ

ファイル追加後に仮想メディアが最新の情報に更新されない

仮想メディア ドライブがマウントされた後、そのドライブにファイルを追加した場合、ターゲット サーバ側でそのファイルがすぐに表示されないことがあります。表示するには、仮想メディア接続をいったん解除し、再確立します。

仮想メディアの Linux ドライブが 2 回リストされる

KX III では、ユーザが Linux™ クライアントに root ユーザとしログインしている場合、ドライブが [Local Drive] (ローカル ドライブ) ドロップダウン リストに 2 回リストされます。

たとえば、eg /dev/sdc と eg /dev/sdc1 が表示されます。1 つ目のドライブはブート セクタ、2 つ目のドライブはディスクの最初のパーティションです。

Windows 2000 の仮想メディアへのアクセス

D2CIM-VUSB を使用して Windows 2000® サーバ上の仮想メディアに仮想メディア ローカル ドライブにアクセスすることはできません。

Mac および Linux の仮想メディア USB ドライブの切断

Linux® または Mac® 環境の場合:

- Linux ユーザに対して、/dev/sdb および /dev/sdb1 が存在している場合、クライアントでは /dev/sdb1 のみが使用され、それがリムーバブル ディスクとして公開されます。
- /dev/sdb をユーザが利用することはできません。
- Linux ユーザに対して、/dev/sdb は存在するけれども /dev/sdb1 がない場合は、/dev/sdb がリムーバブル デバイスとして使用されます。
- Mac ユーザに対しては、/dev/disk1 および /dev/disk1s1 が使用されます。

仮想メディア機能利用時におけるターゲット サーバの BIOS の起動時間

ターゲット サーバにおいてメディアが仮想マウントされている場合、そのターゲット サーバの BIOS の起動に要する時間が長くなることがあります。

▶ 起動に要する時間を短縮するには

1. VKC を終了し、仮想メディア ドライブを完全に解放します。
2. ターゲット サーバを再起動します。

高速の仮想メディア接続を使用した場合の仮想メディアの接続エラー

[High Speed USB] (高速 USB) 接続でターゲットに問題が発生する場合、またはターゲットで接続やケーブルの追加に起因する信号劣化により USB プロトコル エラーが発生する場合は、[Use Full Speed for Virtual Media CIM] (仮想メディア CIM でフル スピードを使用) の選択が必要になることがあります。（たとえば、ドングルを介したブレード サーバへの接続)。

USB ポートおよびプロファイルに関する留意事項

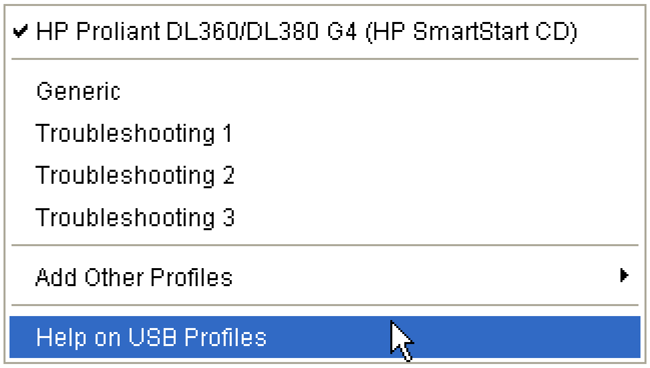
VM-CIM および DL360 の USB ポート

HP® DL360 サーバの背面と前面には、USB ポートがそれぞれ 1 つあります。DL360 では、両方の USB ポートを同時に使用することはできません。つまり、DL360 サーバに対してデュアル VM-CIM を使用することはできません。

ただし、代替策として、DL360 サーバの背面の USB ポートに USB2 ハブを接続し、そのハブにデュアル VM-CIM を接続することはできます。

USB プロファイルの選択に関するヘルプ

Virtual KVM Client (VKC) で KVM ターゲット サーバに接続しているとき、[USB Profile] (USB プロファイル) メニューの [Help on USB Profiles] (USB プロファイルに関するヘルプ) をクリックすると、USB プロファイルに関する情報が表示されます。



USB プロファイルに関するヘルプは、[USB Profile Help] (USB プロファイルに関するヘルプ) ウィンドウに表示されます。個々の USB プロファイルの詳細については、「選択可能な USB プロファイル」を参照してください。

サーバで使用されている多様な OS および BIOS に対応する USB プロファイルが、標準で用意されています。このため、リモート USB デバイスとターゲット サーバを最適な方法で対応付けることができます。

"Generic" プロファイルは、一般に使用されているほとんのターゲット サーバ構成のニーズに対応しています。

その他のプロファイルは、一般的に展開される他のサーバ設定 (例: Linux® や Mac OS X®) の特定のニーズを満たすように提供されています。

さらに、ターゲット サーバが BIOS レベルで動作しているときなどに仮想メディア機能の互換性を高めるための、さまざまなプロファイルが用意されています (プロファイルの名前がプラットフォーム名と BIOS のリビジョンで構成されている)。

[Add Other Profiles] (他のプロファイルを追加) をクリックすると、システムで使用可能なその他のプロファイルが一覧表示されます。この一覧で設定したプロファイルは、[USB Profile] (USB プロファイル) メニューに追加されます。この一覧には、トラブルシューティング用プロファイルのセットがあります。これらのプロファイルは、構成における制限事項を明確化するのに役立ちます。

[USB Profile] (USB プロファイル) メニューの項目を変更するには、KX III ローカル コンソールまたは KX III リモート コンソールの [Device Settings] (デバイス設定) メニューの [Port Configuration] (ポート設定) ページを使用します。

Raritan から提供されている標準の USB プロファイルがどれもターゲット サーバの要件を満たさない場合、Raritan のテクニカル サポート部門がお客様と協力し、そのターゲット サーバに対する解決策を探ることができます。次の手順を実行することを推奨します。

1. Raritan の Web サイト (www.raritan.com) の [Firmware Upgrade] (ファームウェアのアップグレード) ページで最新のリリース ノートを調べ、ご使用のターゲット サーバ構成に合った解決策が提供されているかどうかを確認します。
2. 提供されていない場合は、Raritan のテクニカル サポート部門に問い合わせます。その際、次の情報を準備してください。
   a. ターゲット サーバに関する情報 (製造元、モデル、BIOS、およびバージョン)。
   b. 用途 (例: イメージをリダイレクトし、サーバの OS を CD-ROM から再ロードする)。

スマート カード リーダー使用時の USB プロファイルの変更

ターゲット サーバの USB プロファイルの変更が必要になる場合があります。たとえば、接続速度が [High Speed USB] (高速 USB) のときにターゲットに問題が発生する場合、接続速度を [Use Full Speed for Virtual Media CIM] (仮想メディア CIM でフル スピードを使用) に変更する必要があります。

プロファイルを変更すると、「新しいハードウェアが検出されました」というメッセージが表示されることがあります。この場合は、管理者権限でターゲットにログインして USB ドライバを再インストールする必要があります。この現象は、ターゲットで USB デバイスの新しい設定が検出される最初の数回だけ発生する可能性があります。その後はターゲットによって正しいドライバが選択されます。

ビデオ モードと解像度に関する留意事項

Mac でのビデオ画像の表示が暗い場合

Mac® の HDMI ビデオ ポートを使用していて、ビデオが暗すぎる場合は、CIM の DVI 互換モードを有効にすると、問題の解決に役立ちます。

「*CIM ポートの設定* 『*94*p. 』」を参照してください。

ローカル ポートで黒色の縞が表示される場合

特定のサーバおよび画面解像度では、ローカル ポートで画面の端に黒色の小さい縞が表示される場合があります。

このような場合は、以下の手順に従います。

1. 別の解像度を設定してみます。または、
2. デジタル CIM を使用している場合は、[Port Configuration] (ポート設定) ページで [Display Native Resolution] (本来の表示解像度) を別の解像度に変更します。あるいは、
3. HDMI CIM を使用している場合は、DVI 互換モードにします。

さらに支援を必要とする場合は、Raritan のテクニカル サポートにお問い合わせください。

Sun Composite Sync ビデオ

Sun™ Composite Sync ビデオは、サポートされていません。

SUSE と VESA のビデオ モード

SUSE の X.org 設定ツールである SaX2 を実行すると、X.org 設定ファイル内の Monitor セクションの Modeline エントリにビデオ モードが書き込まれます。これらのビデオ モードは、VESA モニタを選択している場合であっても、VESA のビデオ モード タイミングと正確に対応していません。一方 KX III では、正確に同期させるため、VESA のビデオ モード タイミングが使用されています。このビデオ モード タイミングの不一致により、黒の境界線が表示される、画面の一部が表示されない、ノイズが発生する、などの問題が発生することがあります。

► **SUSE のビデオ表示を設定するには**

1. 生成された設定ファイル /etc/X11/xorg.conf 内に Monitor セクションがあり、その中に UseModes というオプションがあります。たとえば、
   UseModes "Modes[0]" と書き込まれています。
2. この行の先頭に # を付加してコメント行にするか、または、この行全体を削除します。
3. X サーバを再起動します。

これにより、X サーバの内部ビデオ モード タイミングが使用されるようになるので、VESA のビデオ モード タイミングと正確に対応します。この結果、KX III 経由で画面が正しく表示されます。

キーボードに関する留意事項

フランス語キーボード

キャレット記号 (Linux クライアントのみ)

Linux® クライアントとフランス語キーボードを併用する場合、Virtual KVM Client (VKC) では Alt Gr + 9 というキー組み合わせがキャレット記号 (ˆ) として処理されません。

► **キャレット記号を入力するには**

フランス語キーボードの ˆ キー (P キーの右にある) を押し、すぐに Space キーを押します。

次のコマンドを実行するマクロを作成する方法もあります。

1. 右 Alt キーを押す。
2. 9 キーを押す。
3. 9 キーを離す。
4. 右 Alt キーを離す。

注:これらの手順は、母音の上に付ける曲折アクセントには当てはまりません。フランス語キーボードで ^ キーと他の文字を組み合わせて使用した場合、曲折アクセントになります。

アクセント記号 (Windows XP クライアントのみ)

Windows XP® クライアントでフランス語キーボードを使用する場合、Virtual KVM Client (VKC) で Alt Gr + 7 というキー組み合わせを使用すると、アクセント記号付き文字が 2 つ表示されます。

注:この現象は、Linux® クライアントでは発生しません。

数字キーパッド

Virtual KVM Client (VKC) でフランス語キーボードを使用する場合、数字キーパッドにある記号は次のとおりに表示されます。

数字キーパッド上の記号キー	表示
/	;
.	;

ティルデ記号

Virtual KVM Client (VKC) でフランス語キーボードを使用する場合、Alt Gr + 2 というキー組み合わせがティルデ記号 (~) として処理されません。

▶ ティルデ記号を入力するには

次のコマンドを実行するマクロを作成します。

- 右 Alt キーを押す。
- 2 キーを押す。
- 2 キーを離す。
- 右 Alt キーを離す。

キーボード言語の設定 (Fedora クライアント)

Linux® 版の JRE™ には、[System Preferences] (システム基本設定) で設定した外国語キーボードに対して正しいキー イベントが生成されない、という問題があります。したがって、次の表に示す方法を使用して外国語キーボードを設定することを推奨します。

言語	設定方法
アメリカ英語/国際	デフォルト設定
イギリス英語	[System Settings] (システム設定) (Control Center)
フランス語	Keyboard Indicator
ドイツ語	Keyboard Indicator
ハンガリー語	[System Settings] (システム設定) (Control Center)
スペイン語	[System Settings] (システム設定) (Control Center)
ドイツ語 (スイス)	[System Settings] (システム設定) (Control Center)
ノルウェー語	Keyboard Indicator
スウェーデン語	Keyboard Indicator
デンマーク語	Keyboard Indicator
日本語	[System Settings] (システム設定) (Control Center)
韓国語	[System Settings] (システム設定) (Control Center)
スロベニア語	[System Settings] (システム設定) (Control Center)
イタリア語	[System Settings] (システム設定) (Control Center)
ポルトガル語	[System Settings] (システム設定) (Control Center)

注:デスクトップ環境として Gnome を使用している Linux システムでは、Keyboard Indicator を使用してください。

Linux クライアントでハンガリー語キーボードを使用している場合、ダブル アキュート付き U およびダブル アキュート付き O は、JRE 1.6 (以降) でのみ入力できます。

Fedora® クライアントでは、キーボード言語を設定する方法がいくつかあります。Virtual KVM Client (VKC) でキーを正しく対応付けるには、次に示す方法を使用する必要があります。

▶ [System Settings] (システム設定) を使用してキーボード言語を設定するには

1. ツールバーで [System] (システム) > [Preferences] (基本設定) > [Keyboard] (キーボード) を選択します。
2. [Layouts] (レイアウト) タブをクリックします。
3. 言語を追加または選択します。
4. [Close] (閉じる) をクリックします。

▶ Keyboard Indicator を使用してキーボード言語を設定するには

1. タスク バーを右クリックし、[Add to Panel] (パネルに追加) をクリックします。
2. [Add to Panel] (パネルに追加) ダイアログ ボックスで、Keyboard Indicator を右クリックし、メニューの [Open Keyboard Preferences] (キーボード基本設定) をクリックします。
3. [Keyboard Preferences] (キーボード基本設定) ダイアログ ボックスで、[Layouts] (レイアウト) タブをクリックします。
4. 必要に応じて言語を追加または削除します。

Linux ターゲット サーバでマクロが保存されない場合

Linux® Fedora™ 18 と Java™ 1.7.0 (update 45 以降) が稼働しているターゲット サーバでマクロを作成して保存しても、次のエラー メッセージが表示される場合は、ターゲット サーバで Fedora 18 の SELinux を無効にして問題を解決してください。

"An error occurred attempting to write the new keyboard macros. (キーボード マクロを新規作成しようとして、エラーが発生しました。) Macro was not added (マクロは追加されませんでした)"

リモート アクセスに対応していない Mac キーボードのキー

クライアントとして Mac® を使用している場合、Mac® キーボードの次のキーは、Java™ Runtime Environment (JRE™) によって取り込まれません。

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

その結果、Virtual KVM Client (VKC) では、Mac クライアントのキーボードのこうしたキーは処理できません。

マウスに関する留意事項

マウス ポインタの同期 (Fedora)

Fedora® 7 を実行しているターゲット サーバにデュアル マウス モードで接続しているときに、ターゲット サーバとローカルのマウス ポインタが同期しなくなった場合、マウス モードをインテリジェント モードに、またはインテリジェント モードから標準モードに変更すると同期が回復することがあります。

シングル マウス モードを使用すると、制御しやすくなります。

▶ マウス ポインタを再度同期させるには、以下の手順に従います。

- Virtual KVM Client (VKC) の [Synchronize Mouse] (マウスを同期) オプションを使用します。

シングル マウス モード: CC-SG の管理下にあるターゲットに接続する場合

Firefox® と DCIM-PS2 または DCIM-USBG2 を使用して、CC-SG の管理下にある KX III ターゲットに接続しているとき、Virtual KVM Client (VKC) でシングル マウス モードに切り替えると、VKC ウィンドウからフォーカスが外れ、マウスが応答しなくなります。

この場合、マウスの左ボタンをクリックするかまたは Alt キーを押しながら Tab キーを押し、フォーカスを VKC ウィンドウに戻します。

音声

音声の再生とキャプチャに関する問題

音声接続を妨げる可能性がある機能

音声デバイスに接続中、以下の機能を使用している場合は、音声接続が妨げられる可能性があります。音声デバイスに接続する場合は、これらの機能を使用しないことを推奨します。

- ビデオの自動検出
- ローカル ポートを頻繁に使用する機能
- ユーザの追加

キャプチャ デバイスおよび再生デバイスをターゲットで同時に使用した場合の問題

一部のターゲットでは、USB ハブ コントローラーとその USB ポートの管理方法により、キャプチャ デバイスと再生デバイスの同時接続が機能しない場合があります。必要な帯域幅が小さい音声形式を選択することを検討してください。

それでも問題が解決しない場合は、ターゲットで D2CIM-DVUSB CIM のキーボードおよびマウス コネクタを別のポートに接続してください。それでも問題が解決しない場合は、デバイスを USB ハブに接続し、ハブをターゲットに接続してください。

Linux 環境での音声

以下は、Linux® 環境で音声機能を使用する場合の既知の問題です。

- Linux® ユーザは、再生にデフォルト音声デバイスを使用してください。デフォルト以外のサウンド カードを選択した場合は、音が出力されない可能性があります。
- SuSE 11 クライアントでは、YAST を介して Javas_1_6_0-sun-alsa (ALSA 対応の java-1_6_0-sun) をインストールしておく必要があります。
- マイクが組み込まれた Logitech® ヘッドセットの場合は、[Mono Capture] (モノラル キャプチャ) オプションのみを使用できます。
- デバイスを表示するためには、SUSE 11 および ALSA ドライバを実行している場合、KX III からログアウトして、ログインし直します。

  また、音声デバイスの接続と切断を数回繰り返した場合、本来は 1 回だけリストされるべきデバイスが、複数回リストされる可能性があります。
- Fedora Core® 13 ターゲットで音声機能を使用している場合、モノラル 16 ビット、44k に設定すると、再生が著しく妨げられる可能性があります。

Windows 環境での音声

Windows® 64 ビットクライアントで、Virtual KVM Client (VKC) からデバイスにアクセスすると、[Connect Audio] (音声に接続) パネルに再生デバイスが 1 つだけリストされます。

音声デバイスはデフォルト デバイスであり、[Connect Audio] (音声に接続) パネルに「Java Sound Audio Engine」として表示されます。

スマート カードに関する留意事項

Fedora サーバへの Virtual KVM Client (VKC) スマート カードの接続

Virtual KVM Client (VKC) でスマート カードを使用して Linux® Fedora® サーバに接続する場合は、pcsc-lite ライブラリを 1.4.102-3 以降にアップグレードします。

CC-SG に関する留意事項

VKC のバージョンが CC-SG プロキシ モードで認識されない

Virtual KVM Client (VKC) を CommandCenter Secure Gateway (CC-SG) からプロキシ モードで起動した場合、VKC のバージョンは認識されません。

[About Raritan Virtual KVM Client] (VKC のバージョン情報) ダイアログ ボックスで、バージョンが "Version Unknown" (不明なバージョン) と表示されます。

デバイスのポート間の移動

同じ Raritan デバイスのポート間で移動し、1 分以内に管理作業を再開した場合、CC-SG によってエラー メッセージが表示されることがあります。

管理作業を再開すると、最新の情報に更新されます。

ブラウザに関する留意事項

Fedora 使用時の Firefox のフリーズに関する問題の解決

Fedora® サーバを使用している場合に Firefox® にアクセスすると、Firefox を開くときに Firefox がフリーズすることがあります。

この問題を解決するには、libnpjp2.so という Java™ プラグインをサーバにインストールします。

Ap F　　FAQ

この章の内容

一般的な FAQ... 377
リモート アクセス 380
ユニバーサル仮想メディア... 384
帯域幅と KVM-over-IP のパフォーマンス...................................... 386
IPv6 ネットワーキング 390
サーバ... 392
ブレード サーバ... 393
インストール.. 395
ローカル ポート － KX III.. 397
拡張ローカル ポート 399
二重化電源.. 399
インテリジェント電源タップ（PDU）の管理 400
Ethernet と IP ネットワーキング... 401
ローカル ポートの統合およびカスケード接続 403
コンピュータ インタフェース モジュール（CIM)............................ 406
セキュリティ 407
スマート カード認証と CAC 認証.. 409
管理機能 410
ドキュメントおよびサポート 412
その他... 413

一般的な FAQ

質問	回答
Dominion KX III とは何ですか?	Dominion KX III は第 3 世代のデジタル KVM (キーボード、ビデオ、マウス) スイッチです。1、2、4、または 8 人の IT 管理者は BIOS レベルの機能を使用して、ネットワーク上の 8、16、32、または 64 台のサーバにアクセスし、そのサーバを制御できます。Dominion KX III ではハードウェアと OS が完全に独立しているため、サーバがダウンしているときでも、ユーザはトラブルシューティングや再設定を行えます。 ラックからアクセスする場合も Dominion KX III では従来のアナログ KVM スイッチと同様の機能性と利便性が提供され、スペースやコストを削減できます。その一方、Dominion KX III には業界最高のパフォーマンスを誇る KVM-over-IP 技術も組み込まれているため、複数の管理者がネットワーク接続されたワークステーション、iPhone®、iPad® からサーバ KVM コンソールにアクセスできます。

質問	回答
KX III は、KX II とどう違うのですか？	KX III は、KX II の次世代バージョンです。処理能力とストレージが増強された最新のハードウェア設計を特徴とする KX III では、IT 管理向けの KVM-over-IP アクセス、およびブロードキャスト アプリケーション向けの高パフォーマンスの IP アクセスが実現されます。KX III には、X II のほぼすべての機能と、以下の先進技術が組み込まれています。 KX III の新しいビデオ処理エンジンでは、従来のコンピュータ アプリケーションから、30 フレーム/秒、1920 x 1080 ビデオ、24 ビット カラー、デジタル音声、デュアル モニタ、および DVI、HDMI、DisplayPort、VGA ビデオを必要とするダイナミックなブロードキャスト アプリケーションに至るまで、幅広いアプリケーションがサポートされています。 業界初の DVI ベースのローカル ポートを備えた KX III の共通ユーザ インタフェースにより、ローカル管理およびサーバ アクセスに関してこれまでにない生産性やパフォーマンスが得られます。 すべての KX III モデルにカスケード接続ポートが装備されているため、複数の Dominion KX III を接続し、それぞれに接続されたサーバへのアクセスが可能になります。統合ポート リスト経由で最大 1024 台のサーバにアクセスできます。 KX III は、KX II でサポートされていたすべての Dominion CIM および Paragon II CIM をサポートします。

質問	回答
Dominion KX III がリモート制御ソフトウェアと異なるのは、どのような点ですか?	Dominion KX III をリモートで使用すると、インタフェースは一見 pcAnywhere™、Windows® Terminal Services/Remote Desktop、VNC などのリモート制御ソフトウェアと同じに見えます。しかし Dominion KX III はソフトウェアではなく、ハードウェア ソリューションであるため、より強力な機能を提供します。 ハードウェアや OS に依存しない: Dominion KX III を使用して、一般的なさまざまな OS が稼動しているサーバ、たとえば、Windows、Linux®、Solaris™ などが稼動する Intel®、Sun®、PowerPC を搭載したサーバを管理できます。 状態に依存せず、エージェントも不要 - Dominion KX III では、管理サーバで OS を起動している必要がありません。さらに、管理サーバに特別なソフトウェアをインストールする必要もありません。 アウトオブバンド – 管理サーバ自身のネットワーク接続が利用できない場合でも、Dominion KX III を経由して管理できます。 BIOS レベルのアクセス - サーバが起動時に停止した場合や、セーフ モードでの起動が必要な場合、またはシステム BIOS パラメータの変更が必要な場合でも、Dominion KX III は問題なく動作し、これらの設定を行えます。
Dominion KX III をラックにマウントすることができますか?	使用できます。Dominion KX III には、標準 19 インチ ラック マウント ブラケットが同梱されています。また、逆向きに収容して、サーバ ポートがある面を前にすることもできます。
Dominion KX III のサイズはどのくらいですか?	Dominion KX III の高さはわずか 1U であり (2U である KX3-864 および KX3-464 を除く)、標準の 19 インチ ラックに収容できます。奥行きはわずか 29 cm です。Dominion KX3-832 および KX3-864 の奥行きは 36 cm です。

リモート アクセス

質問	回答
Dominion KX III ごとに何人のユーザがサーバにリモート アクセスできますか？	Dominion KX III モデルでは、ユーザ チャネルごとに最大 8 人のユーザが 1 台のターゲット サーバに同時にリモート アクセスし、そのターゲット サーバを制御することができます。DKX3-116 のような 1 チャネルのデバイスの場合、最大 8 人のリモート ユーザが 1 台のターゲット サーバにアクセスして制御することができます。DKX3-216 のような 2 チャネルのデバイスの場合は、チャネル 1 で最大 8 人のユーザがあるターゲット サーバにアクセスして制御し、また、チャネル 2 で別の最大 8 人のユーザが別のターゲット サーバにアクセスして制御することができます。4 チャネルのデバイスの場合は、チャネルごとに最大 8 人のユーザ（合計で 8 x 4 = 32 人のユーザ）が、最大 4 台のターゲット サーバにアクセスし、それらのターゲット サーバを制御することができます。同様に、8 チャネルのデバイスの場合は、最大 8 人のユーザが 1 台のターゲット サーバにアクセスし、8 チャネルで最大 32 人のユーザがターゲット サーバにアクセスできます。
iPhone または iPad からリモートでサーバにアクセスできますか。	使用できます。KX III に接続されているサーバに iPhone または iPad からアクセスできるようになりました。
2 人のユーザが同じターゲット サーバの画面を同時に表示できますか。	使用できます。最大 8 名のユーザが 1 台のサーバに同時にアクセスし、制御できます。
2 人のユーザが同じターゲット サーバにアクセスするとき、一方のユーザがリモートでアクセスし、もう一方のユーザがローカル ポートからアクセスすることはできますか。	使用できます。ローカル ポートはリモート ″ポート″ からは完全に独立しています。PC 共有機能を使用することで、ローカル ポートから同じサーバにアクセスできます。

質問	回答
クライアントから Dominion KX III にアクセスする場合、どのようなハードウェア、ソフトウェア、ネットワーク設定が必要ですか？	Dominion KX III は Web アクセスが可能なため、アクセスするための特別なソフトウェアをお客様がクライアントにインストールする必要はありません
	注:リリース KX III 3.0.0 では、モデムがサポートされていませんが、今後のリリースでサポートされる予定です。
	Dominion KX III には、以下の主要な Web ブラウザを使用してアクセスできます。Internet Explorer® および Firefox® を使用してアクセスできます。Dominion KX III には、Windows®、Linux®、および Mac® デスクトップで、Raritan の Windows クライアントおよび Java™ ベースの Virtual KVM Client™ からアクセスできます。 Dominion KX III 管理者は、便利なブラウザベースのインタフェースを使用して、リモート管理 (パスワードとセキュリティの設定、サーバ名の変更、IP アドレスの変更など) を行うこともできます。

<table>
<tr><th>質問</th><th>回答</th></tr>
<tr><td>Dominion KX III へのアクセスに使用されるアプレットのファイル サイズはどのくらいですか？また、この VKC アプレットを取得するのにどのくらいの時間がかかりますか。</td><td>Dominion KX III へのアクセスに使用される Virtual KVM Client (VKC) アプレットのサイズは約 500 キロバイトです。以下の表に、Dominion KX III のアプレットの取得に必要な時間をネットワークの速度ごとに示します。
<table>
<tr><td>100 Mbps</td><td>100 Mbps ネットワークの理論上の速度</td><td>0.05 秒</td></tr>
<tr><td>60 Mbps</td><td>100 Mbps ネットワークの実効速度</td><td>0.08 秒</td></tr>
<tr><td>10 Mbps</td><td>10 Mbps ネットワークの理論上の速度</td><td>0.4 秒</td></tr>
<tr><td>6 Mbps</td><td>10 Mbps ネットワークの実効速度</td><td>0.8 秒</td></tr>
<tr><td>512 Kbps</td><td>標準的なケーブルモデムのダウンロード速度</td><td>8 秒</td></tr>
</table></td></tr>
<tr><td>Windows KVM クライアントは用意されていますか。</td><td>使用できます。Raritan Active KVM Client (AKC) というネイティブの .NET Windows クライアントが用意されています。「Active KVM Client (AKC) ヘルプ 『294p. 』」を参照してください。</td></tr>
<tr><td>Windows 以外の KVM クライアントは用意されていますか。</td><td>使用できます。Virtual KVM Client (VKC) では、Windows 以外のユーザがデータ センタのターゲット サーバに接続できます。「Virtual KVM Client (VKC) ヘルプ 『242p. 』」を参照してください。</td></tr>
<tr><td>KVM クライアントは多言語対応ですか。</td><td>使用できます。Dominion KX III のリモート HTML ユーザ インタフェースおよび KVM クライアントでは、日本語、簡体中国語、繁体中国語に対応します。スタンドアロンでも CC-SG 経由でも多言語をサポートします。</td></tr>
</table>

質問	回答
KVM クライアントにおいてデュアル液晶モニタはサポートされていますか。	使用できます。机上で複数台の液晶モニタを使用して生産性を向上させたいお客様のために、Dominion KX III では複数台のモニタに対して KVM セッションを確立できるようになっています。全画面モードと標準モードのどちらも使用できます。
ビデオ カードを 2 枚搭載したサーバをサポートしますか。	はい。リモート ユーザが利用可能な拡張デスクトップ設定で、ビデオ カードが 2 枚サポートされています。

ユニバーサル仮想メディア

質問	回答
Dominion KX III のどのモデルで仮想メディアがサポートされていますか？	すべての Dominion KX III モデルで仮想メディアがサポートされています。スタンドアロンでも、Raritan の集中管理アプライアンスである CommandCenter® Secure Gateway を通じても使用できます。
Dominion KX III では、どのタイプの仮想メディアがサポートされていますか？	Dominion KX III では、以下のタイプのメディアがサポートされています。内蔵または USB 接続された CD/DVD ドライブ、USB 接続された大容量ストレージ デバイス、PC の内蔵ハード ディスク、および ISO イメージです。

質問	回答
仮想メディアに必要なものは何ですか。	Dominion KX III 用の仮想メディア CIM が必要です。VGA ベースの 2 つの CIM として、D2CIM-VUSB および D2CIM-DVUSB があります。 D2CIM-VUSB には USB コネクタが 1 つあり、仮想メディアを OS レベルで利用したいお客様に適しています。 D2CIM-DVUSB には USB コネクタが 2 つあり、仮想メディアを BIOS レベルで利用したいお客様に適しています。D2CIM-DVUSB は、スマート カード認証、カスケード接続、デジタル音声にも必要です。 どちらの CIM でも、USB 2.0 インタフェースに対応しているターゲット サーバへの仮想メディア セッションがサポートされています。32 個セットおよび 64 個セットのお得な CIM パッケージが用意されています。これらの CIM でも、ずれないマウス (Absolute Mouse Synchronization™) やリモート ファームウェア更新がサポートされています。 弊社の CIM は、従来からアナログ VGA ビデオをサポートしています。3 つの新しいデュアル仮想メディア CIM では、DVI、HDMI、DisplayPort などのデジタル ビデオ形式をサポートしています。この新しい CIM には、D2CIM-DVUSB DVI、D2CIM-DVUSB HDMI、および D2CIM-DVUSB DP があります。
仮想メディアは安全ですか。	使用できます。仮想メディアのセッションは、256 ビットの AES、128 ビットの AES または RC4 暗号化によって保護されます。
仮想メディアは実際に音声をサポートしていますか。	使用できます。音声の再生と Dominion KX III に接続されたサーバへの録音が可能です。データセンタ内のリモート サーバで再生するサウンドや音声を、デスクトップ PC またはラップトップに接続したスピーカーを使用して聞くことができます。また、PC またはラップトップに接続したマイクを使用してリモート サーバに録音することもできます。デジタル CIM または D2CIM-DVUSB デュアル仮想メディア CIM が必要です。

質問	回答
USB プロファイルとは何ですか。	一部のターゲット サーバでは、仮想メディアなど USB ベースのサービスを利用するために、特別に構成された USB インタフェースを必要とします。USB プロファイルは、KX III の USB インタフェースをターゲット サーバの特性に合わせて調整するものです。
USB プロファイルを使用するのはなぜですか。	USB プロファイルは、BIOS レベルで特に必要となります。仮想メディア ドライブにアクセスする際、BIOS レベルでは USB 仕様が完全にサポートされていないことがあります。一方、USB プロファイルは OS レベルで使用されることもあります。たとえば、Macintosh サーバや Linux サーバにおいてマウス動作を同期させる場合などです。
USB プロファイルはどのように使用しますか。	管理者は KX III の [Port Configuration] (ポート設定) ページで、特定の USB プロファイルを使用するように個々のポートまたはポート グループを設定できます。必要があれば、USB プロファイルを KX III クライアントで選択することもできます。詳細については、ユーザ ガイドを参照してください。
仮想メディアを利用する際、USB プロファイルを必ず設定する必要がありますか。	いいえ。仮想メディアを OS レベルで利用する場合や、仮想メディアにアクセスせずに BIOS レベルで操作する場合、デフォルトの USB プロファイルで十分なケースがほとんどです。
使用可能なプロファイルはどれですか。詳細情報はどこで入手できますか。	使用できるプロファイルや詳細については、ユーザ ガイドを参照してください。

帯域幅と KVM-over-IP のパフォーマンス

質問	回答
KVM-over-IP システムで使用される帯域幅はどのくらいですか。	Dominion KX III のまったく新しいビデオ処理により、ビデオの柔軟性とパフォーマンスが向上し、帯域幅を効率的に利用でき、LAN、WAN、またはインターネット経由でいつでも、どこにでもアクセスできます。 Dominion KX III では、ターゲット サーバからのキーボード、ビデオ、およびマウス信号のデジタル化、圧縮、および暗号化が行われ、IP ネットワーク経由でリモート クライアントに IP パケットが送信され、ユーザへのリモート セッションが形成されます。KX III は業界最高水準のビデオ処理アルゴリズムを備えているので、ローカル アクセスする場合と遜色ない画質が得られます。 画面が変更される際、帯域幅の大部分が使用されるので、キーボードとマウスの処理に割り当てられる帯域幅がかなり狭くなります。 重要なのは、帯域幅はユーザがアクティブであるときにのみ使用される、という点です。使用される帯域幅は、サーバの画面表示の変更量に基づいて決まります。 画面が変更されない場合、つまり、ユーザがサーバとの間で対話操作をしていない場合、一般に帯域幅はほとんどまたはまったく使用されません。ユーザがマウスを動かした場合やキーボードで文字を入力した場合、少量の帯域幅が使用されます。複雑なスクリーン セーバを実行している場合や動画を再生している場合、多量の帯域幅が使用される可能性があります。
帯域幅は KVM-over-IP システムのパフォーマンスにどのような影響を及ぼしますか。	一般に、帯域幅とパフォーマンスはトレードオフの関係にあります。使用できる帯域幅が広いほど、パフォーマンスが向上します。帯域幅に制約のある環境では、パフォーマンスが低下するおそれがあります。Dominion KX III は、多種多様な環境で高いパフォーマンスを得られるように最適化されています。

質問	回答
帯域幅に影響を及ぼす要素は何ですか。	帯域幅の使用量を決める要素はいろいろあります。最大の要素は前述のとおり、ターゲットサーバの画面表示の変更量です。画面表示の変更量は、ユーザの操作内容によって異なります。 その他の要素としては、サーバの画面解像度、ネットワークの速度と特性、KVM Client の接続プロパティ、クライアント PC のリソース、ビデオ カードのノイズなどがあります。
KX III で一般的な作業を行う際に使用される帯域幅はどのくらいですか？	使用帯域幅は、主にユーザの操作内容によって決まります。画面表示の変更量が多いほど、使用される帯域幅も広くなります。

質問	回答
パフォーマンスおよび帯域幅を最適化するにはどうすればよいですか？	KX III の、ユーザ向けのリモート クライアントでさまざまな設定を行うことにより、帯域幅とパフォーマンスを最適化できます。デフォルト設定では、標準の LAN/WAN 環境において、ローカル アクセスする場合と同等のパフォーマンスが得られると共に、使用帯域幅が節約されます。 **[Optimize For] (最適化):** この設定で、標準の IT /コンピュータ アプリケーションまたはビデオ/ブロードキャスト アプリケーションのビデオ エンジンを設定します。 **[Compression] (圧縮):**スライダを左に動かすとビデオ品質が最高になり、右に動かすと帯域幅が最小になります。 **[Noise Filter] (ノイズ フィルタ):** ほとんどの場合、デフォルトの設定で効果を発揮しますが、レスポンシブ ビデオの場合は左に動かし、低帯域幅の場合は右に動かすことができます。 その他に帯域幅を狭くするためのヒントとして、以下の方法があります。 ▪ デスクトップの壁紙に､複雑な画像ではなく無地の画像を使用する。 ▪ スクリーンセーバを無効にする。 ▪ ターゲット サーバで低いビデオ解像度を使用する。 ▪ Windows のコントロール パネルの［画面］で、［ドラッグ中にウィンドウの内容を表示する］チェック ボックスをオフにする。 ▪ シンプルな画像、テーマ (例: Windows クラシック)、およびデスクトップを使用する
インターネット経由で接続したいと考えています。どの程度のパフォーマンスが期待できますか。	パフォーマンスは、リモート クライアントと KX III の間のインターネット接続の帯域幅と伝送遅延によって決まります。ケーブル モデム接続または高速 DSL 接続の場合、LAN/WAN 接続に近いパフォーマンスが得られる可能性があります。低速ネットワークの場合は、前述の推奨値に設定し、パフォーマンスを向上させてください。

質問	回答
帯域幅の広い環境で KX III を使用することを検討しています。パフォーマンスを最大化するにはどうすればよいですか。	デフォルト設定で十分に機能します。[Connection Properties] (接続プロパティ) 設定を左に動かすと、ビデオ パフォーマンスを高めることができます。
IP ネットワーク上でのリモート アクセスにおいてサポートされている最大ビデオ解像度はどのくらいですか。	Dominion KX III は、フル HD リモート画面解像度 (1920 x 1080、フレーム レート: 最大 30 フレーム/秒、デジタル音声付き) をサポートしている、業界初かつ唯一の KVM-over-IP スイッチです。 また、よく使われる横長画面形式 (例: 1600 x 1200、1680 x 1050、1440 x 900) もサポートされているので、リモート ユーザは最近販売されている高解像度モニタを使用できます。
音声はどれくらいの帯域幅を使用しますか。	使用する音声形式のタイプにもよりますが、CD 品質の音声を聞く場合は、約 1.5 Mbps が使用されます。
DVI ポート搭載サーバはどのように接続できますか。	DVI-A (アナログ) と DVI-I (アナログ/デジタル統合) をサポートする DVI ポートを備えたサーバでは、Raritan の低価格の ADVI-VGA パッシブ アダプタを使用して、サーバの DVI ポートを VGA プラグに変換し、KX III CIM の VGA プラグに接続できます。 DVI-I または DVI-D (デジタル) をサポートする DVI ポートを搭載したサーバでは、新しい D2CIM-DVUSB DVI CIM を使用できます。

IPv6 ネットワーキング

質問	回答
IPv6 とは何ですか。	IPv6 は "Internet Protocol Version 6" の頭字語です。IPv6 は次世代の IP プロトコルであり、現在使用されている Internet Protocol Version 4 (IPv4) プロトコルを置き換えるものです。 IPv6 は、IPv4 が抱えているさまざまな問題を解決します (例: IPv4 アドレスの枯渇)。 経路選択やネットワーク自動設定などの機能が IPv4 よりも向上しています。IPv6 は徐々に IPv4 を置き換えていくと予想されています。つまり、数年間は両者が共存することになります。 管理者の観点から見ると、IPv6 は IP ネットワークの大きな問題の 1 つを解消します。その問題とは、IP ネットワークの設定作業と保守作業です。
KX III で IPv6 ネットワーキングがサポートされているのはなぜですか?	米国のさまざまな政府機関と国防総省は、調達時に IPv6 対応製品を購入するよう義務付けられています。また、多くの企業および国 (例: 中国) が、今後数年間で IPv6 に移行する予定です。
デュアル スタックとは何ですか。また、デュアル スタックが必要なのはなぜですか。	デュアル スタックとは、IPv4 と IPv6 のプロトコルを同時にサポートする機能のことです。IPv4 から IPv6 に徐々に移行していくことを考えると、デュアル スタックは IPv6 をサポートするうえで必須機能であると言えます。
KX III 上で IPv6 を有効にするにはどうすればよいですか?	[Device Settings] (デバイス設定) タブから [Network Settings] (ネットワーク設定) ページを開きます。次に、[IPv6 Address] (IPv6 アドレス) チェック ボックスをオンにし、[IP Auto Configuration] (IP 自動設定) ボックスの一覧で値を選択します。詳細については、ユーザ ガイドを参照してください。
IPv6 アドレスが設定された外部サーバがあります。この外部サーバを KX III と併用する場合、どうなるでしょうか?	KX III から外部サーバ (SNMP マネージャ、syslog サーバ、LDAP サーバなど) の IPv6 アドレスを使用してそうしたサーバにアクセスすることができます。 具体的に言うと、KX III のデュアル スタック アーキテクチャを使用することにより、IPv4 アドレス、IPv6 アドレス、またはホスト名を指定してこれらの外部サーバにアクセスすることができます。つまり KX III は、今後多くのお客様の社内で発生する IPv4/IPv6 混在環境に対応できます。

質問	回答
社内ネットワークで IPv6 がサポートされていない場合、どうなるでしょうか?	KX III は、出荷時設定では IPv4 だけを使用するようになっています。社内ネットワークで IPv6 を使用できる状態になったら、前述の「Dominion KX II 上で IPv6 を有効にするにはどうすればよいですか。」の手順を実行し、IPv4/IPv6 デュアル スタックを有効にします。
IPv6 に関する詳細情報はどこで入手できますか。	www.ipv6.org に、IPv6 に関する全般情報が掲載されています。また、KX III のユーザ ガイドでは、KX III における IPv6 のサポートについて説明されています。

サーバ

質問	回答
Dominion KX III の操作は Windows サーバに依存しますか?	必要ありません。ユーザは、どのようなシナリオでも必ず使用できる KVM インフラストラクチャに依存しているため (問題を解決するために KVM インフラストラクチャを使用するような場面も考えられます)、Dominion KX III は外部サーバからも完全に独立するよう設計されています。
Dominion KX III に接続するには、サーバでどのような準備が必要ですか?	理想的なマウス同期を実現し、画面表示に影響するスクリーンセーバや電源管理の機能をオフにするように、マウス パラメータ オプションを設定します。
マウス同期機能はどのようになっていますか。	これまでの KVM-over-IP のマウス同期は、不満が残るものでした。Dominion KX III には「ずれないマウス」機能が備わっています。これにより、Windows サーバまたは Apple® Mac サーバを使用している場合は、サーバ側のマウス設定を変更することなく、マウスの動きを厳密に同期させることができます。その他のサーバの場合は、インテリジェント マウス モードまたは高速なシングル マウス モードを使用すれば、サーバ側のマウス設定を変更せずに済みます。

質問	回答
Dominion KX III には何が同梱されていますか？	次のアイテムが同梱されています。(1) Dominion KX III ユニット、(2) クイック セットアップ ガイド、(3) 標準 19 インチ ラック マウント ブラケット、(4) ユーザ マニュアル CD-ROM、(5) 使用地域の AC ライン コード、(6) 保証書とその他の文書。

ブレード サーバ

質問	回答
ブレード サーバを Dominion KX III に接続できますか？	使用できます。Dominion KX III では、代表的なブレード サーバ メーカー (HP®、IBM®、Dell®、および Cisco®) の主要なブレード サーバ モデルがサポートされています
サポートされているブレード サーバはどれですか。	サポートされているモデルは次のとおりです。Dell PowerEdge® 1855、1955、および M1000e、HP BladeSystem c3000 と c7000、IBM BladeCenter® H、E、および S、Cisco UCS B-Series。
どの CIM を使用すればよいですか。	使用する CIM は、ご使用のブレード サーバの製造元とモデルにおける KVM ポートのタイプによって決まります。サポートされている CIM は、DCIM-PS2、DCIM-USBG2、D2CIM-VUSB、および D2CIM-DVUSB です。
使用可能なアクセスおよび制御の方法はどれですか。	Dominion KX III では、(1) ローカル ポートからアクセス、(2) IP を使用してリモート アクセス、(3) CC-SG 経由でアクセス、(4) モデムを使用してアクセス、という 4 種類の方法により、自動で安全な KVM アクセスが可能です。
複数台のブレード サーバを切り替える際、ホットキーを使用する必要がありますか。	一部のブレード サーバでは、複数台のブレード サーバを切り替える際にホットキーを使用する必要があります。Dominion KX III では、ホットキーを使用する必要はありません。ブレード サーバの名前をクリックするだけで、自動的にそのブレード サーバに切り替わります。ホットキーを明示的に使用する必要はありません。

質問	回答
ブレード サーバの管理モジュールにアクセスできますか。	使用できます。管理モジュールの URL を定義し、Dominion KX III または CommandCenter Secure Gateway からアクセスすることができます。ワンクリック アクセスが設定されている場合、1 回のクリック操作でアクセスできます。
Dominion KX III には何台のサーバを接続できますか？	パフォーマンス上および信頼性上の理由により、1 台の Dominion KX III に接続できるブレード シャーシは、モデルにかかわらず最大 8 台です。接続するブレード サーバ筐体の台数は、KX III でサポートされているリモート接続数の 2 倍以内にすることを推奨します。たとえば、リモート チャネルが 2 本ある KX3-216 の場合、接続するブレード サーバ シャーシを 4 台以内にすることをお勧めします。もちろん、残りのサーバ ポートにブレード サーバを接続することもできます。
当社は大企業であり、CommandCenter Secure Gateway を使用しています。CommandCenter Secure Gateway からブレード サーバにアクセスできますか。	使用できます。Dominion KX III 上でブレード サーバの設定が完了したら、CommandCenter Secure Gateway から KVM 接続を使用してブレード サーバにアクセスできるようになります。さらに、ブレード サーバは、シャーシ別に CommandCenter Secure Gateway のカスタム ビューにも表示されます。
インバンド KVM アクセスまたは埋め込み KVM アクセスも必要な場合はどうなりますか。	ブレード サーバに対するインバンド アクセスおよび埋め込みアクセスは、CommandCenter Secure Gateway で設定できます。
一部のブレード サーバ上で VMware® を実行しています。この構成はサポートされていますか。	使用できます。CommandCenter Secure Gateway を使用して、ブレード サーバ上で実行されている仮想マシンを表示し、また、その仮想マシンにアクセスすることができます。
仮想メディアはサポートされていますか。	これは、ブレード サーバによって異なります。HP ブレードは、仮想メディアをサポートできます。IBM BladeCenter (BladeCenter T 以外) は、適切に設定されている場合には仮想メディアをサポートします。仮想メディア CIM (D2CIM-VUSB または D2CIM-DVUSB) を使用する必要があります。

質問	回答
ずれないマウス機能はサポートされていますか。	ブレード筐体内に KVM スイッチを備えているサーバの場合、通常、ずれないマウス機能はサポートされません。HP ブレードおよび Dell の一部のブレード サーバの場合は、CIM を各ブレードに接続できるので、ずれないマウス機能がサポートされます。
ブレード サーバへのアクセスは安全ですか。	使用できます。ブレード サーバへのアクセスには、Dominion KX III の標準的なセキュリティ機能（128 ビットまたは 256 ビットの暗号化など）がすべて使用されます。その他、ブレード サーバ特有のセキュリティ機能があります。たとえば、ブレード サーバごとにアクセス権限を付与する機能や、入力されたホットキーを拒否する機能などがあるので、不正アクセスの防止に役立ちます。
Dominion KSX II および KX III-101 で、ブレード サーバはサポートされていますか？	現時点では、これらの製品ではブレード サーバはサポートされていません。

インストール

質問	回答
Dominion KX III を設置するには、ユニット本体のほかに何を Raritan に注文する必要がありますか？	Dominion KX III に接続するサーバごとに、サーバのキーボード、ビデオ、マウス ポートに直接接続するアダプタである Dominion または Paragon コンピュータ インタフェース モジュール（CIM）が必要です。
導入時、どのタイプの Cat5 ケーブルを使用すればよいですか。	Dominion KX III では、Cat5、Cat5e、または Cat6 の標準 UTP (非シールド ツイスト ペア) ケーブルを使用できます。Raritan のマニュアルや販売資料では、単に「Cat5」と記載されています。実際には、Dominion KX III にはどのブランドの UTP ケーブルも使用できます。

質問	回答
Dominion KX III には、どのタイプのサーバおよび PC を接続できますか?	Dominion KX III はサーバのベンダを選びません。標準に準拠したキーボード ポート、ビデオ ポート、およびマウス ポートを搭載しているあらゆるサーバを接続できます。さらに、シリアル ポートを搭載したサーバは、P2CIM-SER CIM を使用して管理できます。
どのようにサーバを Dominion KX III に接続すればよいですか?	Dominion KX III に接続するサーバには、サーバのキーボード ポート、ビデオ ポート、マウス ポートに直接接続する Dominion CIM または Paragon CIM が必要です。Cat5、Cat5e、Cat6 などの標準 UTP (非シールド ツイスト ペア) ケーブルを使用して、各 CIM を Dominion KX III に接続します。
サーバは、Dominion KX III からどのくらいの距離に設置できますか?	サーバの種類にもよりますが、一般に、サーバは Dominion KX III から最大で 45 m (150 フィート) 離れた場所に設置できます (詳細については、「***ターゲット サーバのサポートされている画面解像度、接続距離、およびリフレッシュ レート*** 『*337*p. 』」を参照してください)。仮想メディアとずれないマウスをサポートしている D2CIM-VUSB CIM の場合、推奨範囲は 30 m (100 フィート) です。
オペレーティング システムによっては、操作中にキーボードかマウスを切断した場合、システムがロックする場合があります。それらを切断しても Dominion KX III に接続しているサーバがロックしないようにするには、どうすればよいですか?	Dominion コンピュータ インターフェース モジュール (DCIM) ドングルは、それぞれ接続されているサーバに対する仮想キーボードや仮想マウスとして動作します。この技術は、KME (キーボード/マウス エミュレーション) と呼ばれます。Raritan の KME 技術は、データ センタでの使用に耐えるグレードであり、厳正にテストされています。また、ローエンドの KVM スイッチの技術に比べてはるかに高い信頼性が確保されています。この技術には 15 年間以上に及ぶ実績も生かされており、世界中で何百万台ものサーバに実装されています。
Dominion KX III に接続されているサーバには何らかのエージェントをインストールする必要がありますか?	Dominion KX III はハードウェアを介してサーバのキーボード用、ビデオ用、マウス用の各ポートに直接接続されるため、Dominion KX III に接続されたサーバには、ソフトウェア エージェントを一切インストールする必要がありません。

質問	回答
Dominion KX III ユニットごとに何台のサーバを接続できますか?	Dominion KX III モデルでは、1U シャーシの場合は 8、16、または 32 個のサーバ ポートを、2U シャーシの場合は 8 ～ 64 個のサーバ ポートが用意されています。このデジタル KVM スイッチ ポートの密度は、業界の最高水準です。
サーバを Dominion KX III から切断して別の Dominion KX II に再接続した場合、または同じ Dominion KX III ユニットの別のポートに接続した場合、どうなりますか?	サーバ接続先ポートを変更した場合、サーバ ポート名が自動更新されます。この変更内容は、ローカル クライアントおよびすべてのリモート クライアントに反映されます。CC-SG を使用している場合は、CC-SG にも反映されます。
Cisco のルータやスイッチ、Sun ヘッドレス サーバなど、シリアル制御 (RS-232) デバイスは、どのように Dominion KX III に接続すればよいですか?	シリアル制御デバイスの数が少ない場合は、Raritan の P2CIM-SER シリアル変換器を使用して Dominion KX III に接続できます。 お客様は、Dominion KSX II (KVM およびシリアルの統合スイッチ) の導入を検討することもできます。DKSX-144 は、4 つの KVM-over-IP ポートおよび 4 つのシリアル ポートを装備しています。 DKSX-188 は、8 つの KVM-over-IP ポートおよび 8 つのシリアル ポートを装備しています。 ただし、シリアル制御デバイスの数が多い場合は、Raritan のセキュア コンソール サーバである Dominion SX 製品を使用することをお勧めします。Dominion SX は、Dominion KX III よりも割安な価格で、より優れたシリアル機能を提供できます。この SX は使いやすく、設定や管理が簡単であるうえに、展開している Dominion シリーズと完全に統合できます。

ローカル ポート - KX III

質問	回答
ラックからサーバに直接アクセスできますか。	使用できます。Dominion KX III は、ラックで従来の KVM スイッチと同じように機能し、1 組のキーボード、モニタ、マウスを使用して、最大 64 台のサーバを制御できます。ブラウザベースのユーザ インターフェイスまたはホットキーによってサーバを切り替えることができます。
複数台の KX III のローカル ポートを統合できますか？	使用できます。KX III のカスケード接続機能を利用すれば、複数台の KX III のローカル ポートを別の KX III に接続できます。これにより、データ センタ内の 1 か所から統合ポート リストを使用して、KX III に接続されているサーバにアクセスできます。
自分がローカル ポートを使用しているとき､他ユーザがサーバにリモート アクセスできないように設定できますか。	いいえ。Dominion KX III のローカル ポートには、サーバへの完全に独立したアクセス パスがあります。つまり、ユーザーはラックからサーバにローカル アクセスできます。ラックに同時にリモート アクセスするユーザーの数を制限する必要はありません。
USB キーボードまたは USB マウスをローカル ポートで使用できますか。	使用できます。Dominion KX III ローカル ポートエリアには､USB キーボード ポートおよびマウス ポートがあります。Dominion KX III には、PS/2 ローカルポートはありません。PS/2 のキーボードおよびマウスを使用しているお客様は、PS/2－USB アダプタを利用する必要があります。
ローカル アクセスする場合、オンスクリーン ディスプレイ（OSD）は表示されますか。	表示されます。ただし、Dominion KX III のラックからのアクセスは、従来の OSD よりもはるかに優れています。Dominion KX III にはローカル アクセス用に業界初のブラウザベースのインタフェースが実装されされています。また、ローカル ポートではローカル アクセスとリモート アクセスに同じインタフェースが使用されます。さらに、大半の管理機能をローカルで実行できます。
ローカル ポートを使用しているとき､サーバを切り替えるにはどうすればよいですか。	ローカル ポートを使用しているとき、接続されているサーバが、リモート クライアントと同じ画面に表示されます。サーバを切り替えるには、切り替え先サーバをマウスでクリックするか、ホットキーを使用します。

質問	回答
承認されたユーザだけがローカル ポートからサーバにアクセスできるようにするには、どうすればよいですか。	ユーザがローカル ポートを使用するには、リモートでアクセスする場合と同レベルの認証を受ける必要があります。これは次のことを意味します。 Dominion KX III が外部 RADIUS、LDAP、または Active Directory® サーバと連動するよう設定している場合、ユーザがローカル ポートへのアクセスを試みると、同じサーバで認証されます。 外部認証サーバが利用できない場合は、Dominion KX III は自身の内部認証データベースにフェイルオーバします。 Dominion KX III は独自のスタンドアロン認証を備えているため、即座にインストールを有効にできます。

拡張ローカル ポート

質問	回答
拡張ローカル ポートとは何ですか。	Dominion KX2-808、KX2-832、および KX2-864 には、拡張ローカル ポートが搭載されています。対応する Dominion KX III モデルには、拡張ローカル ポートがありません。代わりに、すべての KX III モデルには、カスケード接続ポートが搭載されています。 KX III のデジタル ローカル ポートを拡張する場合は、Raritan Cat5 Reach DVI 製品を使用すると、500 メートルまでのローカル アクセスおよびリモート アクセスが可能になります。 「*KX III と Cat5 Reach DVI の接続 - 拡張ローカル ポート機能の提供* 『*312*p. 』」を参照してください。

二重化電源

質問	回答
Dominion KX III には二重化電源オプションがありますか?	使用できます。Dominion KX III の全モデルは、AC 入力と AC 電源が二重化されており、自動フェイルオーバ機能を備えています。KX III では一方の電源入力や電源に障害が発生すると、もう一方に自動的に切り替えられます。
Dominion KX III で使用する電源では、電圧設定が自動検知されますか?	使用できます。Dominion KX III の電源は、100 ～ 240 V、50 ～ 60 Hz の範囲の AC 電圧で使用できます。
電源または入力電力に障害が発生した場合、通知されますか。	電源障害は Dominion KX III の前面パネルにある LED でユーザに通知されます。同時に、エントリも監査ログに送信され、KX リモート クライアント ユーザ インタフェースに表示されます。管理者によって設定されている場合は、その後 SNMP イベントまたは syslog イベントが発生します。

インテリジェント電源タップ (PDU) の管理

質問	回答
Dominion KX III にはどのようなタイプのリモート電源管理機能が用意されていますか?	Raritan のインテリジェント PDU は、ターゲット サーバやその他の機器の電源を管理するために Dominion KX III に接続できます。サーバの場合は、簡単な設定作業を一度行えば、サーバ名をクリックするだけで電源を投入または切断したり、停止したサーバに電源を再投入したりできます。
Dominion KX III ではどのようなタイプの電源タップがサポートされていますか?	Raritan の Dominion PX™ 電源タップおよび Remote Power Control (RPC) 電源タップ。 この電源タップには、さまざまなコンセント、コネクタ、およびアンペアの製品があります。PM シリーズの電源タップはコンセントレベルで切り替えできないので、こうした電源タップを Dominion KX III に接続しないでください。
Dominion KX III ユニットには何台の PDU を接続できますか?	1 台の Dominion KX III に最大 8 台の PDU を接続できます。

質問	回答
PDU をどのように Dominion KX III に接続すればよいですか?	電源タップを Dominion KX III に接続するには、D2CIM-PWR を使用します。D2CIM-PWR は別途購入する必要があります。PDU には付属していません。
Dominion KX III では、複数の電源を持つサーバはサポートされていますか?	使用できます。Dominion KX III では、複数の電源タップに接続された複数の電源でサーバをサポートするよう簡単に設定できます。ターゲット サーバごとに 4 つの電源を接続できます。
Dominion KX III には PDU の統計情報と測定値が表示されますか?	使用できます。PDU レベルの電源統計情報 (例: 電力、電流、電圧) が PDU から取得され、ユーザに対して表示されます。
リモート電源管理では、接続されているサーバを特別に設定する必要がありますか。	一部のサーバでは、電源をいったん切断して再投入したときにサーバが自動再起動しないように、BIOS が設定されています。このようなサーバを使用する場合、そのサーバのドキュメントを読み、この設定を変更してください。
サーバの電源を入れ直すとどうなりますか。	これは、サーバの AC 電源コードをいったん抜いて再度差し込むのと同じことです。

Ethernet と IP ネットワーキング

質問	回答
Dominion KX III の Ethernet インタフェースの速度はどのくらいですか?	Dominion KX III では、10/100 Ethernet に加えてギガビット Ethernet もサポートされています。Dominion KX III では 2 つの 10/100/1000 Ethernet インタフェースがサポートされており、速度と二重化の設定を変更できます (自動検知または手動で設定)。
ワイヤレス接続で Dominion KX III にアクセスできますか?	使用できます。Dominion KX III は標準の Ethernet を使用するだけでなく、高品質なビデオ表示を保ちつつ、使用する帯域幅を抑えます。そのため、ワイヤレス クライアントを Dominion KX III にネットワーク接続していても、サーバの BIOS レベルの設定と管理をワイヤレスで行えます。

質問	回答
Dominion KX III には、冗長フェイルオーバまたは負荷分散を行うためのデュアル ギガビット Ethernet ポートが用意されていますか？	使用できます。Dominion KX III には、冗長フェイルオーバ機能を実現するためのデュアル ギガビット Ethernet ポートが搭載されています。プライマリ Ethernet ポート（またはポートに接続されているスイッチやルータ）に障害が発生した場合、Dominion KX III が同じ IP アドレスを持つセカンダリ ネットワーク ポートにフェイルオーバすることにより、サーバの動作が中断されないようにします。自動フェイルオーバは、管理者が有効にする必要があります。
Dominion KX III を VPN で使用できますか？	使用できます。Dominion KX III では、レイヤ 1 ～ 4 において標準的なインターネット プロトコル（IP）技術が使用されています。そのため、標準的な Virtual Private Network（VPN）から届いたトラフィックを簡単にトンネリングできます。
KX III とプロキシ サーバを組み合わせて使用できますか？	使用できます。リモート クライアント PC が適切に設定されている場合、KX III を SOCKS プロキシ サーバと組み合わせて使用することができます。詳細については、ユーザ マニュアルまたはオンライン ヘルプを参照してください。
Dominion KX III にネットワーク アクセスできるようにするためには、ファイアウォールで TCP ポートをいくつ開く必要がありますか？	2 つのポートが必要です。TCP ポート 5000 で他の Dominion デバイスを検知して Raritan デバイスと CC-SG 間の通信を行います。また、もちろんポート 443 で HTTPS 通信を行います。
また、これらのポートは変更できますか。	使用できます。Dominion KX III の TCP ポートは管理者が設定できます。
Dominion KX III は Citrix® と共に使用できますか？	設定を適切に行えば、Dominion KX III を Citrix などのリモート アクセス製品と共に使用できます。ただし、Raritan では十分なパフォーマンスを維持しつつ作業できるかどうかは保証できません。Citrix のような製品は、デジタル KVM スイッチと概念が似ているビデオ リダイレクト技術が使用されています。したがって、併用した場合 2 種類の KVM-over-IP 技術が同時に使用されるという点にご注意ください。

質問	回答
Dominion KX III では DHCP を使用できますか？	DHCP アドレス割り当ては使用できますが、Raritan では固定 IP アドレスの設定を推奨しています。Dominion KX III はインフラストラクチャ デバイスであるため、固定 IP アドレスを使用した方が、Dominion KX III に対してより効率的にアクセスし、管理できます。
IP ネットワークから Dominion KX III にアクセスできなくなりました。原因は何でしょうか。	Dominion KX III はお客様の LAN または WAN ネットワークに依存しています。考えられる原因は次のとおりです。 Ethernet のオートネゴシエーション。ネットワークによっては、10/100 オート ネゴシエーションが適切に機能しないため、Dominion KX III ユニットを 100 Mb/全二重に設定するか、ネットワークに最適な設定を行う必要があります。 IP アドレスの重複。Dominion KX III の IP アドレスが他のデバイスと 重複していると、ネットワーク接続を確立できない場合があります。 ポート 5000 の競合。他のデバイスでポート 5000 を使用している場合は、Dominion KX III のデフォルト ポートを変更する必要があります (または、他のデバイスのポートを変更する必要があります)。 Dominion KX III の IP アドレスを変更するか、新しい Dominion KX II に切り替える場合、KX III の IP アドレスと Mac® アドレスがレイヤ 2、レイヤ 3 のネットワークに通知されるまで、十分な時間が必要です。

ローカル ポートの統合およびカスケード接続

質問	回答
複数の Dominion KX III を 1 つのソリューションとして統合するには、物理的にどのように接続すればよいですか？	複数台の KX III を互いに物理接続してローカル アクセスを統合するには、KX III のカスケード接続ポートを使用して、カスケード接続された複数台の KX III の接続ポートをベース KX III に接続します。これにより、データ センタ内の 1 か所から統合ポート リストを使用して、KX III に接続されているサーバにアクセスできます。 カスケード接続された KX III をベース KX III に接続するには、カスケード接続ポートを使用する必要があります。 統合ポート リストを使用したアクセスは、データ センタ内だけでなくリモート PC からでも可能です。階層型ポート リストまたは検索機能（およびワイルドカード）を使用することにより、カスケード接続 KX III に接続されているすべてのサーバにアクセスできます。 カスケード接続レベルは 2 段階までサポートされています。また、カスケード接続構成内の最大 1,024 個のデバイスにアクセスできます。リモート電源制御もサポートされています。 将来のリリースでは、カスケード接続構成内で仮想メディア、スマート カード、およびブレード サーバへのアクセスがサポートされる予定です。もちろん、これらの機能は標準リモート接続においても利用できます。 利便性を考慮して、IP ネットワーク上で統合ポート リストを使用してリモート IP サーバにアクセスできるようになっています。ただし、CommandCenter から、またはサーバが接続されている KX III からカスケード接続サーバにリモート アクセスする方法の方が、パフォーマンスが高くなるので推奨されます。

質問	回答
Dominion KX III どうしを物理接続する必要がありますか?	複数の Dominion KX III ユニットを物理的に相互接続する必要はありません。その代わりに、各 Dominion KX III ユニットをネットワークに接続します。Raritan の CommandCenter Secure Gateway (CC-SG) 管理アプライアンスを使用して展開すると、1 つのソリューションとして自動的に一体となって機能します。 CC-SG は、リモート アクセスおよびリモート管理用の単一のアクセス ポイントとして機能します。 たとえば、設定作業の集中管理、ファームウェア更新作業の集中管理、認証データベースの一元化などが可能になるので便利です。 リモート アクセスを集中化する目的で CC-SG を使用しているお客様は、KX III のカスケード接続機能を利用することにより、複数台の KX III のローカル ポートを統合し、データ センタ内の 1 か所のコンソールから最大 1,024 台のサーバにローカル アクセスすることができます。
CC-SG は必要ですか。	集中管理システムを使用せずに Dominion KX III をスタンドアロンで使用したいお客様は、従来どおり、複数台の KX III を IP ネットワーク上で相互運用して規模を拡張することになります。複数台の Dominion KX III には、KX III の Web ベースのユーザ インタフェースからアクセスできます。

質問	回答
既存のアナログ KVM スイッチを Dominion KX III に接続できますか？	使用できます。アナログ KVM スイッチは、Dominion KX III のサーバ ポートのいずれかに接続できます。USB コンピュータ インタフェース モジュール (CIM) を使用して、既存のアナログ KVM スイッチのユーザ ポートにつなぐだけです。 ローカル ポートでホットキーベースの切り替えをサポートしているアナログ KVM スイッチを Dominion KX III にカスケード接続すると、統合ポート リストを介してリモートおよびデータ センタを切り替えることができます。 アナログ KVM スイッチの仕様はそれぞれ異なっているため、Raritan では、サードパーティ製の特定のアナログ KVM スイッチについての相互運用性は保証していません。詳細については、Raritan のテクニカル サポート部門にお問い合わせください。

コンピュータ インタフェース モジュール (CIM)

質問	回答
CIM でサポートされているビデオのタイプはどれですか。	弊社の CIM は、従来からアナログ VGA ビデオをサポートしています。3 つの新しい CIM では、DVI、HDMI、DisplayPort などのデジタル ビデオ形式をサポートしています。この新しい CIM には、D2CIM-DVUSB DVI、D2CIM-DVUSB HDMI、および D2CIM-DVUSB DP があります。

質問	回答
Raritan のアナログ マトリックス KVM スイッチである Paragon のコンピュータ インタフェース モジュール (CIM) を Dominion KX III と共に使用できますか?	使用できます。特定の Paragon コンピュータ インタフェース モジュール (CIM) は、Dominion KX III と連動する可能性があります (認定済みの CIM の最新リストについては、Raritan の Web サイトで Dominion KX III リリース ノートを確認してください)。 ただし、Paragon CIM は Dominion KX III CIM より高額のため (最大 304 m (1,000 フィート) のビデオ送信向けの技術が組み込みまれているため)、通常は Dominion KX III 用に Paragon CIM を購入することをお勧めします。また、Paragon CIM を Dominion KX III に接続すると、ビデオ送信距離は Dominion KX III CIM と同じく最大で 46 m (150 フィート) となります。Paragon に接続した場合の 304 m (1,000 フィート) ではありません。
Dominion KX III において Paragon Dual CIM はサポートされていますか?	使用できます。Dominion KX III では、Paragon II Dual CIM (P2CIM-APS2DUAL および P2CIM-AUSBDUAL) がサポートされています。これらの CIM を使用すれば、データ センタ内のサーバを 2 台の異なる Dominion KX III に接続できます。 一方の KX III が使用不能になった場合でも、もう一方の KX III からサーバにアクセスできます。つまり、冗長構成になり、リモート KVM アクセスを二重化できます。 なお、これらは Paragon CIM なので、KX III の拡張機能 (仮想メディア、ずれないマウス、音声など) はサポートされません。

セキュリティ

質問	回答
Dominion KX III は FIPS 140-2 に対応していますか?	Dominion KX III では、FIPS 140-2 実装ガイダンスに従って、Linux プラットフォームで実行されている FIPS 140-2 で検証された埋め込み暗号化モジュールが使用されます。ビデオ、キーボード、マウス、仮想メディア、およびスマート カードのデータで構成される KVM セッション トラフィックの暗号化には、この暗号化モジュールが使用されます。
Dominion KX III ではどのような種類の暗号化が使用されますか?	Dominion KX III の SSL 通信と自身のデータストリームでは、業界標準である極めて安全な 256 ビット AES、128 ビット AES、または 128 ビットの暗号化が使用されます。事実、暗号化によって完全に保護されていないリモート クライアントと Dominion KX III の間ではデータは転送されません。
Dominion KX III では、米国政府の NIST および FIPS 規格で推奨される AES 暗号化がサポートされていますか?	使用できます。Dominion KX III では、セキュリティを高めるために Advanced Encryption Standard (AES) が使用されます。256 ビットおよび 128 ビットの AES を利用できます。 AES は米国政府の承認した暗号アルゴリズムです。NIST (米国の国立標準技術研究所) の FIPS 規格 197 で推奨されています。
Dominion KX III では、ビデオ データの暗号化を行いますか?それとも、キーボードデータとマウス データだけが暗号化されますか。	キーボードとマウスのデータのみを暗号化する競合他社のソリューションとは異なり、Dominion KX III ではセキュリティに関して妥協していません。Dominion KX III では、キーボード、マウス、ビデオ、および仮想メディアのデータの暗号化を行います。
Dominion KX III と、Active Directory、RADIUS、LDAP などの外部認証サーバは、どのように統合して機能しますか?	Dominion KX III には、非常に簡単な設定で、すべての認証要求を LDAP、Active Directory、RADIUS などの外部サーバに転送するよう指定できます。Dominion KX III は、認証されたユーザごとに認証サーバからユーザが属するユーザ グループを受け取ります。次に Dominion KX III は、ユーザが属するユーザ グループに基づいてそのユーザのアクセス許可を決定します。

質問	回答
ユーザ名とパスワードはどのように保存されますか。	Dominion KX III の内部認証機能が使用される場合、ユーザ名やパスワードなどの機密情報はすべて暗号化形式で保存されます。実際に、Raritan のテクニカル サポートやプロダクト エンジニアリング部門を含め、誰もこれらのユーザ名やパスワードを読み出せません。
Dominion KX III では強力なパスワードがサポートされていますか?	使用できます。Dominion KX III には管理者が設定できる強力なパスワード チェック機能があります。この機能によって、ユーザの作成したパスワードが企業または政府の標準を満たし、悪意のあるハッキング行為によって暴かれないようにします。
自社固有のデジタル証明書を Dominion KX III にアップロードできますか?	使用できます。お客様は、自己署名されたデジタル証明書または認証局発行のデジタル証明書を Dominion KX III にアップロードできます。これにより、認証機能を強化し、通信のセキュリティを高めることができます。
Does the KX III ではセキュリティ バナーをカスタマイズできますか?	使用できます。政府機関や軍のようなセキュリティを重視するお客様では、ユーザがログインする前にセキュリティ メッセージを表示する必要があります。KX III では、カスタマイズ可能なバナー メッセージを表示できます。また、このメッセージへの同意を義務付けることもできます。
当社のセキュリティ ポリシーでは、標準の TCP ポート番号の使用を許可していません。TCP ポート番号を変更できますか。	使用できます。セキュリティを強化するために標準の TCP/IP ポート番号を使用したくないお客様の場合、Dominion KX III では管理者が代替ポート番号を設定できるようになっています。

スマート カード認証と CAC 認証

質問	回答
Dominion KX III では、スマート カード認証と CAC 認証はサポートされていますか?	使用できます。ターゲット サーバへのスマート カード認証と DoD Common Access Card (CAC) 認証がサポートされています。

質問	回答
CAC とは何ですか。	Homeland Security Presidential Directive 12 (HSPD-12) によって義務付けられている CAC は、米国政府が作成し、米軍および政府職員が使用するスマート カードの一種です。CAC カードは、多彩な技術に基づく多目的カードであり、識別カードを 1 つにまとめることを目標にしています。詳細については、FIPS 201 規格を参照してください。
スマート カードと CAC がサポートされている KX III のモデルはどれですか？	すべての Dominion KX III モデルでサポートされています。Dominion KX III-101 モデルでは、現在スマート カードと CAC はサポートされていません。
大企業や中小企業でもスマート カードは使用されていますか。	使用できます。なお、スマート カードを最も積極的に導入しているのは米国連邦政府です。
スマート カードと CAC がサポートされている CIM はどれですか。	D2CIM-DVUSB、D2CIM-DVUSB DVI、D2CIM-DVUSB HDMI、D2CIM-DVUSB DP の各 CIM が必要です。
サポートされているスマート カード リーダーはどれですか。	必要なリーダー標準は、USB CCID と PC/SC です。認定済みのリーダーの一覧および詳細については、ユーザ マニュアルを参照してください。
スマート カードと CAC の認証は、ローカル ポートおよび CommandCenter で利用できますか。	使用できます。スマート カードと CAC の認証は、ローカル ポートおよび CommandCenter で機能します。ローカル ポートを使用する場合は、互換性のあるスマート カード リーダーを Dominion KX III の USB ポートに接続します。

管理機能

質問	回答
Dominion KX III は Web ブラウザを介してリモートで管理および設定できますか?	使用できます。Dominion KX III は、Web ブラウザを介して完全にリモートで設定できます。ただし、リモート クライアントに適切なバージョンの Java Runtime Environment (JRE) がインストールされている必要があります。 Dominion KX III の IP アドレスの初期設定のほか、ソリューションの関連事項をすべてネットワーク上で設定できます(実際に、Ethernet クロス ケーブルと Dominion KX III のデフォルト IP アドレスを使用すると、Web ブラウザを介して初期設定も変更できます)。
Dominion KX III の設定のバックアップや復元は可能ですか?	使用できます。非常事態が発生した際に復旧を行うため、Dominion KX III のデバイス設定とユーザ設定は完全にバックアップされます。 Dominion KX III のバックアップ機能と復元機能は、ネットワークや Web ブラウザを介してリモートで使用できます。
Dominion KX III では、どのような監視機能またはログ機能が提供されますか?	ユーザのアカウンタビリティをサポートするため、Dominion KX III では主要なユーザ イベントが日付やタイム スタンプと共に記録されます。記録されるイベントの例としては、ユーザー ログイン、ユーザー ログアウト、特定のサーバへのユーザー アクセス、ログインの失敗、設定の変更など。
Dominion KX III と syslog は一元化できますか?	使用できます。Dominion KX III の独自の内部ログ機能に加え、Dominion KX III ではログ記録されたすべてのイベントを集中 syslog サーバに送信できます。
Dominion KX III と SNMP は一元化できますか?	使用できます。Dominion KX III の独自の内部ログ機能に加え、Dominion KX III では SNMP トラップを SNMP 管理システムに送信できます。SNMP v2 および v3 がサポートされています。
管理者はユーザをログオフすることができますか。	はい。管理者は、どのユーザがどのポートにログインしているかを調べ、必要に応じて特定のポートから、またはデバイスからユーザをログオフすることができます。

質問	回答
Dominion KX III の内部クロックは時刻サーバと同期できますか?	使用できます。Dominion KX III では、企業の時刻サーバとパブリック時刻サーバのいずれかに同期するための業界標準の NTP プロトコルがサポートされています (企業ファイアウォール経由のアウトバウンド NTP リクエストが許可されている場合)。

ドキュメントおよびサポート

質問	回答
オンライン ヘルプは利用できますか。	使用できます。オンライン ヘルプは、ドキュメントと共に raritan.com にあり、KX III ユーザ インタフェースから利用できます。 オンライン ヘルプには、リモート コンソール、Virtual KVM Client (VKC)、Active KVM Client (AKC)、およびローカル コンソールの使用法に関する KX III 管理情報やエンド ユーザ情報、および KX III の仕様、留意事項、KX III と Paragon II の使用法、Cat5 Reach DVI への KX III の接続方法、T1700-LED への KX III の接続方法などが用意されています。
Dominion KX III のドキュメントはどこにありますか?	ドキュメントは、raritan.com にあり、ファームウェア リリース別に一覧表示されています。
どのようなドキュメントを入手できますか。	クイック セットアップ ガイド、オンライン ヘルプ、管理者ガイドやユーザ ガイドの形式でのヘルプの PDF バージョン、リリース ノートなどが用意されています。
特定のサーバにどのような CIM を使用する必要がありますか。	KX III ドキュメントとして用意されている CIM ガイドを調べてください。DVI、HDMI、DisplayPort の各ビデオ規格は、デジタル ビデオ CIM でサポートされています。
KX III のハードウェア保証期間はどのくらいですか?	Dominion KX III の保証期間は標準で 2 年ですが、保証期間を 5 年に延長することもできます。

その他

質問	回答
Dominion KX III のデフォルト IP アドレスは？	192.168.0.192
Dominion KX III のデフォルト ユーザ名とパスワードは？	Dominion KX III のデフォルトのユーザ名とパスワードは「admin/raritan」です（すべて小文字)。ただし、最高レベルのセキュリティを確保するため、Dominion KX III ではユニットが最初に起動した際に、管理者が Dominion KX III のデフォルト管理者ユーザ名とパスワードを変更するよう要求されます。
Dominion KX III の管理者パスワードを変更したところ、新しいパスワードを忘れてしまいました。パスワードを取得してもらえますか？	Dominion KX III では、ハードウェア リセット ボタンを使用してデバイスを工場出荷時の設定に戻すことができます。このとき、デバイスの管理者パスワードもデフォルトのパスワードにリセットされます。
Dominion KX II から Dominion KX III にはどのような方法で移行すればよいですか？	一般に、KX II のお客様には既存のスイッチを長期間お使いいただけます。データ センタを拡張する場合、お客様は新しい KX III モデルを購入して使用することが考えられます。Raritan の集中管理アプライアンスである CommandCenter Secure Gateway (CC-SG) リリース 6.0 は、KX II および KX III をシームレスにサポートします。
現在使用している KX II CIM は、Dominion KX III でも動作しますか？	使用できます。既存の KX II CIM は、Dominion KX III でも動作します。また、KX III で動作する Paragon CIM をお選びください。これにより、KVM over IP への切り替えを検討している Paragon II のお客様は、KX III に簡単に移行できます。ただし、仮想メディア、ずれないマウス機能、および音声をサポートする D2CIM-VUSB CIM および D2CIM-DVUSB CIM を検討することをお勧めします。さらに、DVI、HDMI、および DisplayPort をサポートするデジタル ビデオ CIM も利用できます。

索引

[

[Audit Log] (監査ログ) - 189, 309, 310
[Authentication Settings] (認証設定) - 70
[Auto-sense Video Settings] (ビデオ設定の自動検出) - 256
[Color Accuracy] (色精度) - 246
[Connect] (接続) - 20
[Device Information] (デバイス情報) - 190
[Device Services] (デバイス サービス) - 134
[Disconnect] (切断) - 21
[Encryption & Share] (暗号化および共有) - 176
[Event Management - Destinations] (イベント管理 - 送信先) の設定 - 146, 148, 150, 156
[Event Management - Settings] (イベント管理 - 設定) の設定 - 148, 156
[Firmware Upgrade] (ファームウェアのアップグレード) - 197
[Full Screen Mode] (全画面モード) - 271
[General Settings] (全般) - 263
[Login Limitations] (ログイン制限) - 169, 170
[Network Interface] (ネットワーク インタフェース) ページ - 202
[Network Statistics] (ネットワーク統計) ページ - 202
[Noise Filter] (ノイズ フィルタ) - 247
[Optimize for] (最適化)
選択 - 246
[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ) - 17, 100
[Port Action] (ポート アクション) メニュー - 17, 20, 243, 295
[Port Configuration] (ポート設定) ページ - 90
[Port Configuration] (ポート設定) ページへのアクセス - 89
[Port Type] (ポート タイプ) - 91
[Ports] (ポート) ページに表示されるデュアルポート ビデオ グループ - 233
[Power Cycle] (電源の再投入) - 22
[Power Off] (電源オフ) - 22
[Power On] (電源オン) - 22
[Power Supply Setup] (電源設定) - 157
[Scaling] (拡大、縮小) - 270
[Send Ctrl+Alt+Del] (Ctrl+Alt+Del の送信) マクロ - 250
[Send LeftAlt+Tab] (Send LeftAlt+Tab の送信) - 250
[Send Text to Target] (テキストをターゲットに送信) - 251
[Set Scan] (スキャン設定) タブ - 19
[Strong Passwords] (強力なパスワード) - 83, 170, 172
[Switch From] (切り替え) - 21
[Text Readability] (テキストの読みやすさ) - 246
[Trace Route to Host (ホストへのルートの追跡)] ページ - 205
[USB Profile Management] (USB プロファイルの管理) - 195, 196
[User Management] (ユーザ管理) - 57
[Video Mode] (ビデオ モード) - 246
[View by Group] (グループ別表示) タブ - 19
[View by Search] (検索して表示) タブ - 19
[View Status Bar] (ステータス バーの表示) - 270
[View Toolbar] (ツール バーの表示) - 270
[ホストに ping する] ページ - 205
[ユーザ ブロック] - 170, 174

A

A. AC 電源: - 34
Active KVM Client (AKC) のダイレクト ポート アクセス URL 構文 - 141
Active KVM Client (AKC) ヘルプ - 8, 294, 383
AKC ダウンロード サーバ証明書の検証の有効化 - 143
AKC ダウンロード サーバ証明書の検証を有効にする - 296
AKC ダウンロード サーバ証明書検証の IPv6 サポートに関する留意事項 - 362
AKC でサポートされている Microsoft .Net Framework - 295
AKC でサポートされているオペレーティングシステム - 295
AKC でサポートされているブラウザ - 296

AKC を使用するため前提条件 - 243, 294, 296
Apple Mac のマウス設定 - 33

B

B. ネットワーク ポート - 35

C

C. ローカル ユーザ ポート (ローカル コンソール) - 35
Cat5 Reach DVI の概要 - 312
CC-SG に関する留意事項 - 376
CC-SG ユーザへの注意事項 - 42
CC-SG 管理の終了 - 201
CD-ROM/DVD-ROM/ISO イメージのマウント - 277, 280
CIM アップグレード - 127, 196
CIM キーボード/マウス オプションの設定 - 250
CIM に関する留意事項 - 362
CIM の互換性 - 49
CIM ポートの設定 - 94, 341, 342, 369
CLI コマンド - 214, 219
CLI の画面操作 - 216
CLI プロンプト - 219
CLI を使用した初期設定 - 218
CLI を使用しての KX III へのアクセス - 215
CLI 構文
ヒントとショートカット キー - 217
Cookie を許可 - 296

D

D. ローカル DVI-D ポート - 35
dcTrack での KX III の管理 - 324
dcTrack への KX III のインポート - 327
dcTrack への KX III の追加 - 326
Dell - 101
Dell ブレード シャーシの設定 - 105
Dell 筐体を接続する場合のケーブル長と画面解像度 - 103, 105, 110, 344
DNS の設定 - 39
Dominion KX3-832 - 4
Dominion KX3-864 - 6
DVI モニタへの接続 - 36
DVI 互換モード - 342

E

E. KX III へのターゲット サーバの接続 - 36
Ethernet と IP ネットワーキング - 401

F

F. カスケード接続 (オプション) - 36
FAQ - 377
Fedora サーバへの Virtual KVM Client (VKC) スマート カードの接続 - 376
Fedora 使用時の Firefox のフリーズに関する問題の解決 - 376
FIPS 140-2 サポートの要件 - 181
FIPS 140-2 の有効化 - 178, 180

G

Generic (汎用) - 101

H

HP - 101
HP および Cisco UCS のブレード シャーシ設定 (ポート グループ管理) - 117, 119, 165, 166
HTTP ポートおよび HTTPS ポートの設定 - 134, 354

I

IBM - 101
IBM AIX のマウス設定 - 34
IBM ブレード シャーシの設定 - 110
interface コマンド - 221
IP アクセス制御を設定する - 182
IPv4 の設定 - 37
ipv6 コマンド - 222
IPv6 ネットワーキング - 390
IPv6 のサポートに関する注意事項 - 361
IPv6 の設定 - 38

J

Java Runtime Environment (JRE) に関する留意事項 - 357, 359
Java および Microsoft .NET の要件 - 357
Java が Mac に正しくロードされていない場合 - 360

Java のキャッシュ機能の無効化および Java キャッシュのクリア - 359
Java 検証およびアクセス警告 - 9

K

KVM スイッチを設定する - 93, 135
KVM ポート用のプロファイルの選択 - 56
KX III - KX III 構成の Paragon CIM に関するガイドライン - 319
KX III - Paragon II 構成に関するガイドライン - 320
KX III KVM Client アプリケーション - 8
KX III SNMP トラップのリスト - 151
KX III インタフェースおよびナビゲーション - 16
KX III オンライン ヘルプ - 8
KX III から Paragon II へのアクセス - 316
KX III からターゲット サーバへのアクセス - 43
KX III からのユーザのログオフ (強制ログオフ) - 67, 68, 69
KX III コンソール サーバ設定用コマンドを使用する - 220
KX III コンソールでの案内 - 25
KX III でサポートされているターゲット サーバ画面解像度 - 30, 230, 336, 337
KX III と Cat5 Reach DVI の接続 - 313
KX III と Cat5 Reach DVI の接続 - 拡張ローカル ポート機能の提供 - 1, 312, 399
KX III の MIB の表示 - 145, 148, 154
KX III のアイテム追加要求の送信 - 329
KX III のカスケード接続例 - 137
KX III のデータ サーキットおよび電源サーキットの作成 - 328
KX III のライフサイクルの管理 - 331
KX III の移動 - 331
KX III の再起動 - 199
KX III の使用停止とアーカイブ - 331
KX III の使用停止と保管 - 331
KX III の写真および機能 - 2
KX III の寸法および物理的仕様 - 332
KX III の設置および設定 - 9
KX III の設置と設定 - 9, 28
KX III の前提条件 - 272
KX III の電源オン/オフ - 331
KX III の有効化/有効化 - 331
KX III ファームウェアのアップグレード - 197
KX III への IP アドレスの割り当て - 37
KX III への Paragon II の接続 - 322
KX III への SSH 接続 - 215
KX III へのログイン - 14
KX III ユーザ リストの表示 - 67
KX III リモート コンソール インタフェース - 7, 16
KX III リモート/ローカル コンソール インタフェース - 7
KX III ローカル コンソール - 208
KX III ローカル コンソール - KX III エンドユーザ ヘルプ - 26, 297
KX III ローカル コンソール インタフェース - 7, 26
KX III ローカル コンソール インタフェースへの切り替え - デフォルトのホット キー - 299
KX III ローカル コンソール ファクトリ リセット - 309
KX III ローカル ポートのサポートされている DVI 解像度 - 298, 338
KX III ローカル ポートの設定 - 129, 136
KX III 管理者ヘルプ - 27
KX III 起動中の LED ステータス - 28, 34
KX III 作業工程の管理 - 329
KX III 診断 - 207
KX3-832 の写真 - 4
KX3-832 の特長 - 4
KX3-864 の写真 - 6
KX3-864 の特長 - 6

L

LAN インタフェース設定 - 84, 87, 88
LDAP スキーマを更新する - 234
LDAP/LDAPS から返す場合 - 234
LDAP/LDAPS リモート認証の実装 - 71, 76
Linux クライアントからドライブに接続できない場合 - 364
Linux ターゲット サーバでマクロが保存されない場合 - 373
Linux ターゲット サーバに対して Windows の 3 ボタン マウスを使用する場合 - 362
Linux のマウス設定 - 33
Linux リモート クライアントの要件 - 346
Linux 環境での音声 - 375

Linux 環境での仮想メディア - 279

M

Mac Mini BIOS のキー入力コマンド - 352
Mac および Linux の仮想メディア USB ドライブの切断 - 366
Mac クライアントからファイルの読み書きができない場合 - 364
Mac でのビデオ画像の表示が暗い場合 - 369
Mac の JRE の要件およびブラウザに関する注意事項 - 357
Mac のブート メニュー使用時のマウス モード - 53, 56, 127
Mac 環境での音声 - 350
Mac 環境での仮想メディア - 279
Microsoft Active Directory から返す場合 - 234
Microsoft Active Directory についての注意事項 - 42

N

name コマンド - 222

P

Paragon II と KX III の間でサポートされている接続距離 - 322
PC 共有モードが有効になっている場合の音声接続に関する推奨事項 - 285, 348

R

RADIUS リモート認証の実装 - 76
RADIUS 通信交換仕様 - 80
RADIUS 認証用の Cisco ACS 5.x - 79
root ユーザ権限の要件 - 279

S

SNMP エージェントの設定 - 145, 148
SNMP トラップの設定 - 146, 148
SSH を有効にする - 134
SSL 証明書 - 9, 45, 184
Sun Composite Sync ビデオ - 369
Sun Solaris のマウス設定 - 34
Sun サーバへのアクセス時に使用できる特別なキー組み合わせ - 301
SUSE と VESA のビデオ モード - 370
syslog 設定 - 155

T

TCP ポート 443 - 30
TCP ポート 5000 - 30
TCP ポート 80 - 30

U

UNIX/Linux ワークステーションから SSH で接続する - 215
URL を経由したダイレクト ポート アクセスの有効化 - 140
USB プロファイル - 49, 249, 250
USB プロファイルの設定 ([Port] (ポート) ページ) - 56, 113, 127
USB プロファイルの選択に関するヘルプ - 367
USB ポートおよびプロファイルに関する留意事項 - 367

V

VGA モニタへの接続 (オプション) - 28, 36
Virtual KVM Client (VKC) のダイレクト ポート アクセス URL 構文 - 140
Virtual KVM Client (VKC) ヘルプ - 8, 242, 294, 383
VKC および AKC でのポート スキャンの設定 - 268, 303, 306
VKC のバージョンが CC-SG プロキシ モードで認識されない - 376
VM-CIM および DL360 の USB ポート - 367

W

Web ブラウザ インタフェースの追加に関するヒント - 105, 108, 110, 113, 115, 362
Windows 2000 での複合 USB デバイスの動作 - 363
Windows 2000 のマウス設定 - 32
Windows 2000 の仮想メディアへのアクセス - 366
Windows 7 および Windows Vista のマウス設定 - 32
Windows PC から SSH で接続する - 215
Windows XP 環境での仮想メディア - 278

Windows XP、Windows 2003、Windows 2008 のマウス設定 - 32
Windows キーボードによる Mac ターゲットへのアクセス - 354
Windows 環境での VKC および AKC を介した仮想メディア - 365
Windows 環境での音声 - 376

あ

アクセント記号 (Windows XP クライアントのみ) - 371
アクティブ システム パーティション - 279
アップグレード履歴 - 199
イベント管理 - 148
インストール - 395
インテリジェント マウス モード - 260
インテリジェント マウス モードへの切り替え - 260
インテリジェント マウス同期の条件 - 261
インテリジェント電源タップ (PDU) の管理 - 400
オペレーティング システムの IPv6 のサポートに関する留意事項 - 361
オペレーティング システムの音声再生サポート - 289

か

カスケード接続ターゲットでサポートされていない機能および限定的にサポートされている機能 - 137
カスケード接続デバイス - [Port Access] (ポート アクセス) ページ - 18, 135
カスケード接続デバイスからのリモート アクセスとローカル アクセス - 139
カスケード接続デバイスからの電源制御 - 140
カスケード接続を構成する前に - 136
カスケード接続を設定および有効化する - 36, 135
カスケード接続を有効にする - 136, 138
キーボード - 250
キーボード マクロ - 251
キーボード レイアウト コードの変更 (Sun ターゲット) - 44
キーボードに関する留意事項 - 370
キーボードの制限 - 265
キーボード言語の設定 (Fedora クライアント) - 372
キャビネット正面図およびフロア マップ図での KX III の可視化 - 329
キャビネット内の KX III 用スペースの検索 - 325
キャプチャ/再生バッファ サイズの調整 (音声設定) - 292
キャレット記号 (Linux クライアントのみ) - 370
クライアント コンピュータの仮想メディア ドライブへのアクセス - 276
クライアント起動設定 - 266
グループベースの IP ACL (アクセス制御リスト) - 59, 63, 65, 182
コマンド ライン インタフェース (CLI) - 214
コマンドのオート コンプリート - 216
コンセントとターゲット サーバとの関連付け - 99
コンセントの電源オン/オフの切り替えまたは電源再投入を行う - 47
コンピュータ インタフェース モジュール (CIM) - 406
ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する - 177, 179

さ

サーバ - 392
サポートされていないスマート カード リーダー - 347
サポートされている Paragon II CIMS および設定 - 179, 317
サポートされているオペレーティング システムとブラウザ - 355
サポートされているコンピュータ インタフェース モジュール (CIM) の仕様 - 33, 49, 281, 338
サポートされているスマート カード リーダー - 346
サポートされているデジタル ビデオ CIM (Mac 用) - 340
サポートされているブレード シャーシ モデル - 103, 105, 110, 119
サポートされているプロトコル - 42

サポートされているマウスの追加設定 - 28, 31
サポートされているリモート接続 - 342
サポートされている音声/仮想メディアおよびスマート カード接続の数 - 351
サポートされている音声デバイス形式 - 284, 285
サポートされている仮想メディア オペレーティング システム - 275
サポートされている仮想メディア タイプ - 274
サポートされている仮想メディア ドライブ数 - 275
シングル マウス モード - 263
CC-SG の管理下にあるターゲットに接続する場合 - 374
スキーマ キャッシュを更新する - 238
スキーマへの書き込み操作を許可するようにレジストリを設定する - 235
スクリプトのインポートとエクスポート - 160, 163
スクリプトの接続と切断 - 159
スクリプトの追加 - 160
スクリプトの適用および削除 - 159, 163
スクリプトの変更 - 163
すべての CLI レベルで使用できるコマンド - 217
スマート カード - 281
スマート カード リーダーのアンマウント (取り外し) - 284
スマート カード リーダーのマウント - 283
スマート カード リーダーの検出 - 282
スマート カード リーダーの更新 - 283
スマート カード リーダーへのアクセス時の認証 - 282
スマート カード リーダー使用時の USB プロファイルの変更 - 369
スマート カードに関する留意事項 - 376
スマート カードの最小システム要件 - 281, 307, 344
スマート カードの最小システム要件、CIM、およびサポートされているスマート カード リーダーとサポートされていないスマート カード リーダー - 281
スマート カードの取り外しおよび再挿入の通知の送信 - 284
スマート カード使用時の PC 共有モードおよびプライバシー設定 - 282
スマート カード認証と CAC 認証 - 409
ずれないマウス モード - 260
セキュリティ - 407
セキュリティ バナー - 187
セキュリティと認証 - 209
セキュリティの設定 - 66, 169
セキュリティ警告および検証メッセージ - 9, 10, 14
セキュリティ上の問題 - 169, 220
その他 - 413
その他のセキュリティ警告 - 9, 10
ソフトウェア - 3, 355

た

ターゲット コマンドによるスクリーンショット (ターゲット スクリーンショット) - 258
ターゲット サーバ - 273
ターゲット サーバにアクセスする - 297
ターゲット サーバのサポートされている画面解像度、接続距離、およびリフレッシュ レート - 337, 396
ターゲット サーバの切断 - 44
ターゲット サーバの命名 - 40
ターゲット サーバの要件 - 345
ターゲット サーバへの接続 - 243, 294
ターゲット サーバを切り替える - 43
ターゲット サーバ画面解像度 - 30
ターゲットのスキャン - ローカル コンソール - 306
ダイレクト ポート アクセスおよびデュアル ポート ビデオ グループ - 233
ダイレクト ポート アクセスの有効化 - 142
ツール オプション - 263, 271
ティルデ記号 - 371
デジタル CIM タイミング モード - 341
デジタル CIM の既定モードおよび標準モード - 340, 341
デジタル CIM 既定モード - 341
デジタル CIM 標準モード - 342
デジタル音声 - 284
デジタル音声デバイスの接続 - 289
デジタル音声デバイスの接続および切断 - 288, 289

デバイスのポート間の移動 - 376
デバイスのリセット ボタンによる KX III の リセット - 310
デバイス管理 - 84
デフォルト パスワードを変更する - 37
デフォルトの GUI 言語設定の変更 - 169
デフォルトのログイン情報 - 29
デフォルトの接続プロパティ設定 - 最適化による最高のパフォーマンスの実現 - 245
デュアル スタック ログインのパフォーマンスに関する問題 - 362
デュアル ビデオ サポートに必要な CIM - 225, 284
デュアル ビデオ ポート グループ - 223
デュアル ビデオ ポート グループ - [Port Access] (ポート アクセス) ページ - 18
デュアル ビデオ ポート グループでサポートされているマウス モード - 224, 231, 284
デュアル ビデオ ポート グループの作成 - 141, 142, 165, 167, 223, 231, 233
デュアル ビデオ ポート グループを使用する際の Raritan クライアントの画面操作 - 232
デュアル ビデオ ポート設定手順 - 229
デュアル ポート ビデオ グループの使いやすさに関する注意事項 - 226
デュアル ポート ビデオ グループ設定の例 - 228
デュアル ポート ビデオに関する推奨事項 - 224, 284
デュアル マウス モード - 260
ドキュメントおよびサポート - 412
ドライブ パーティション - 279

な

ネットワーク パラメータの設定 - 218
ネットワークを設定する - 221
ネットワーク基本設定 - 84
ネットワーク設定 - 84, 87, 354
ネットワーク速度の設定 - 88, 342

は

バージョン情報 - Virtual KVM Client - 292
ハードウェア - 2, 332
はじめに - 1
パスワードの変更 - 83
バックアップと復元 - 117, 166, 192
パッケージの内容 - 2
パラメータ値を設定する - 218
ビデオ モードと解像度に関する留意事項 - 298, 369
ビデオのプロパティ - 255
ビデオ設定の調整 - 256
ファイル追加後に仮想メディアが最新の情報に更新されない - 366
ブラウザに関する留意事項 - 376
フランス語キーボード - 370
ブレード サーバ - 393
ブレード シャーシ - [Port Access] (ポート アクセス) ページ - 18
ブレード シャーシ インタフェースへのリンク - 102
ブレード シャーシでサポートされている CIM - 103, 105, 110, 120
ブレード シャーシにアクセスするためのホットキー シーケンス - 102
ブレード シャーシのサンプル URL フォーマット - 107, 112, 114, 125
ブレード シャーシの管理 - 102
ブレード シャーシの手動検出および自動検出の設定 - 101
ブレード シャーシの設定 - 100
ブレード シャーシの必須および推奨設定 - 103, 105, 110, 123
ブレード シャーシ設定オプション - 101
プロファイル名の競合を処理する - 196
ベース デバイスからブレード シャーシへのアクセス - 139
ヘルプでの最新情報 - 1
ポート グループの作成 - 165, 166
ポート グループ管理 - 165
ポート スキャンの設定 - 269
ポート スキャン中のターゲット ステータス インジケータ - ローカル コンソール - 305
ポートからのユーザの切断 - 67, 68, 69
ポートのスキャン - ローカル コンソール - 302
ポートのスキャンのスライド ショー - ローカル コンソール - 303
ポートの設定 - 89
ポート権限の設定 - 59, 62, 65
ポート番号 - 90

ポート別のユーザの表示 - 67, 68
ポート名 - 91
ホット キーと接続キー - 299
ポップアップの許可 - 9

ま

マウス オプション - 259
マウス ポインタの同期 (Fedora) - 374
マウスに関する留意事項 - 374
マウスの設定 - 31
マウスの同期 - 262
マウス同期のヒント - 262
マクロのインポート - 253
マクロのエクスポート - 254
マクロの新規作成 - 251
モデムを設定する - 147
モデルごとにサポートされているユーザ数とポート数 - 7

や

ユーザ - 66
ユーザ グループ - 57
ユーザ グループ リスト - 58
ユーザ グループとユーザの作成 - 42
ユーザ グループ情報を Active Directory サーバから返す - 75
ユーザ グループ情報を RADIUS 経由で返す - 80
ユーザ グループ情報を返す - 234
ユーザ メンバの rciusergroup 属性を編集する - 239
ユーザが同時接続可能 - 298
ユーザとグループの関係 - 58
ユーザ認証プロセス - 82
ユニバーサル仮想メディア - 384

ら

ラック PDU (電源タップ) のコンセントの制御 - 46
ラック PDU (電源タップ) の接続先の設定 - 95
ラック PDU の接続 - 95
ラック PDU の名前の指定 (電源タップの [Port] (ポート) ページ) - 97
ラック マウント - 28
リモート PC - 272
リモート アクセス - 380
リモート アクセスに対応していない Mac キーボードのキー - 374
リモート クライアントの要件 - 346
リモートからのターゲット サーバのアクセスと制御 - 43
ローカル コンソール スキャンの設定 - 268, 303, 306
ローカル コンソールからの KX III ローカルポートの設定 - 209
ローカル コンソールの USB プロファイルオプション - 308
ローカル コンソールのキーボード タイプの選択 - 130, 210
ローカル コンソールのスマート カード アクセス - 281, 307
ローカル コンソールの画面解像度 - 298
ローカル ドライブのマウント - 273
ローカル ドライブのマウントに関する留意事項 - 273
ローカル ポート - KX III - 397
ローカル ポート スキャン モードの設定 - 130
ローカル ポート デバイスのカスケード接続の有効化 - 129, 136
ローカル ポート ホットキーの選択 - 131, 211
ローカル ポートで黒色の縞が表示される場合 - 369
ローカル ポートの統合およびカスケード接続 - 403
ローカル ポートの要件 - 344
ローカル ポート接続キーの選択 - 132, 212
ローカル ユーザ認証の選択 - 133, 213
ログイン - 215, 216

漢字

暗号化および共有の設定 - 176
一般的な FAQ - 377
音声 - 284, 375
音声デバイスの切断 - 291
音声の再生とキャプチャに関する推奨事項と要件 - 285, 289, 348
音声の再生とキャプチャに関する問題 - 375

音声レベル - 285, 348
音声設定の調整 - 292
音声設定の保存 - 288, 289
仮想メディア - 272
仮想メディア ドライブの切断 - 278
仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ) - 280
仮想メディアによりサポートされているタスク - 274
仮想メディアに関する留意事項 - 364
仮想メディアに必要な CIM - 273
仮想メディアの Linux ドライブが 2 回リストされる - 366
仮想メディアの接続および切断 - 276
仮想メディアを使用するための条件 - 272
仮想メディア機能利用時におけるターゲット サーバの BIOS の起動時間 - 366
画面を更新する - 255
概要 - 1, 16, 27, 46, 49, 214, 242, 294, 297, 312, 316, 324, 359
各言語に対して KX III でサポートされているキーボード - 351
拡張ローカル ポート - 399
監査ログおよび Syslog でキャプチャされるイベント - 189, 358
管理機能 - 410
既存の KX III の複製 - 328
既存のユーザ グループの変更 - 65, 69
許可されている KX III カスケード接続構成 - 136
許可の設定 - 60
検出ポートを入力する - 135
権限およびデュアル ビデオ ポート グループ アクセス - 168, 227
個別グループの許可の設定 - 63, 67
後向きの取り付け - 29
高速の仮想メディア接続を使用した場合の仮想メディアの接続エラー - 367
左パネル - 23
左パネルの折りたたみ - 25
仕様 - 332
使用される TCP ポートおよび UDP ポート - 354
使用できる USB プロファイル - 50
手順 1
ターゲット サーバの画面の設定 - 229
ネットワーク ファイアウォールの設定 - 30
手順 2
KVM ターゲット サーバの設定 - 30
KX III へのターゲット サーバの接続 - 230
手順 3
マウス モードおよびポートの設定 - 231
装置の接続 - 34
手順 4
KX III の設定 - 37
デュアル ビデオ ポート グループの作成 - 231
手順 5
KX III リモート コンソールの起動 - 42
デュアル ビデオ ポート グループを開く - 232
手順 6
キーボード言語の設定 (オプション) - 28, 44
手順 7
SSL 証明書の作成およびインストール - 45
手動による dcTrack への KX III の追加 - 326
省電力機能の設定 (オプション) - 133, 213
証明書のインストール - 9, 10
色の調整 - 256
新しい属性を作成する - 235
新規ユーザ グループの追加 - 59
新規ユーザの追加 - 66, 69
診断 - 202
数字キーパッド - 371
接続キーの例 - 132, 212, 299
接続プロパティの概要 - 244
接続プロパティの設定 - 1, 244, 248
接続プロパティへのアクセス - 244
接続情報 - 248
接続情報のアクセスおよびコピー - 245, 249
前向きの取り付け - 28
属性をクラスに追加する - 236
多言語対応キーボードの JRE の要件 - 357
帯域幅と KVM-over-IP のパフォーマンス - 386
帯域幅要件 - 286, 349
単一のリモート クライアントから複数のターゲットへの接続 - 288, 289

電源の関連付け - 99
電源の関連付けの削除 - 99
電源の自動検出の指定 - 40
読み取り/書き込み可能に設定できない状況 - 274, 276
二重化電源 - 399
日付/時刻の設定 - 147, 185
日付/時刻の設定 (オプション) - 41
入門 - 9, 218, 230
汎用ブレード シャーシの設定 - 103
標準ターゲット サーバの設定 - 92
標準マウス モード - 262
標準ローカル ポートの有効化 - 129
表示オプション - 270
保守 - 189
留意事項 - 351, 359
例 1
ブラウザへの証明書のインポート - 11, 14
例 2
[信頼済みサイト] への KX III の追加と証明書のインポート - 13

米国/カナダ/ラテン アメリカ

月曜日～金曜日
午前 8 時～午後 8 時 (米国東海岸時間)
電話 :800-724-8090 または 732-764-8886
CommandCenter NOC に関するお問い合わせ :6 を押してから 1 を押してください。
CommandCenter Secure Gateway に関するお問い合わせ :6 を押してから 2 を押してください。
Fax :732-764-8887
CommandCenter NOC に関する電子メール :tech-ccnoc@raritan.com
その他のすべての製品に関する電子メール :tech@raritan.com

中国

北京

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-10-88091890

上海

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-21-5425-2499

広州

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-20-8755-5561

インド

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+91-124-410-7881

日本

月曜日～金曜日
午前 9 時 30 分～午後 5 時 30 分
電話 : 03-5795-3170
電子メール :support.japan@raritan.com

ヨーロッパ

ヨーロッパ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+31-10-2844040
電子メール :tech.europe@raritan.com

英国

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT)
電話 : +44(0)20-7090-1390

フランス

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+33-1-47-56-20-39

ドイツ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 30 分 (GMT+1 CET)
電話 :+49-20-17-47-98-0
電子メール : rg-support@raritan.com

メルボルン (オーストラリア)

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+61-3-9866-6887

台湾

月曜日～金曜日
午前 9 時～午後 6 時 (標準時 : GMT -5、夏時間 : GMT -4)
電話 :+886-2-8919-1333
電子メール : support.apac@raritan.com